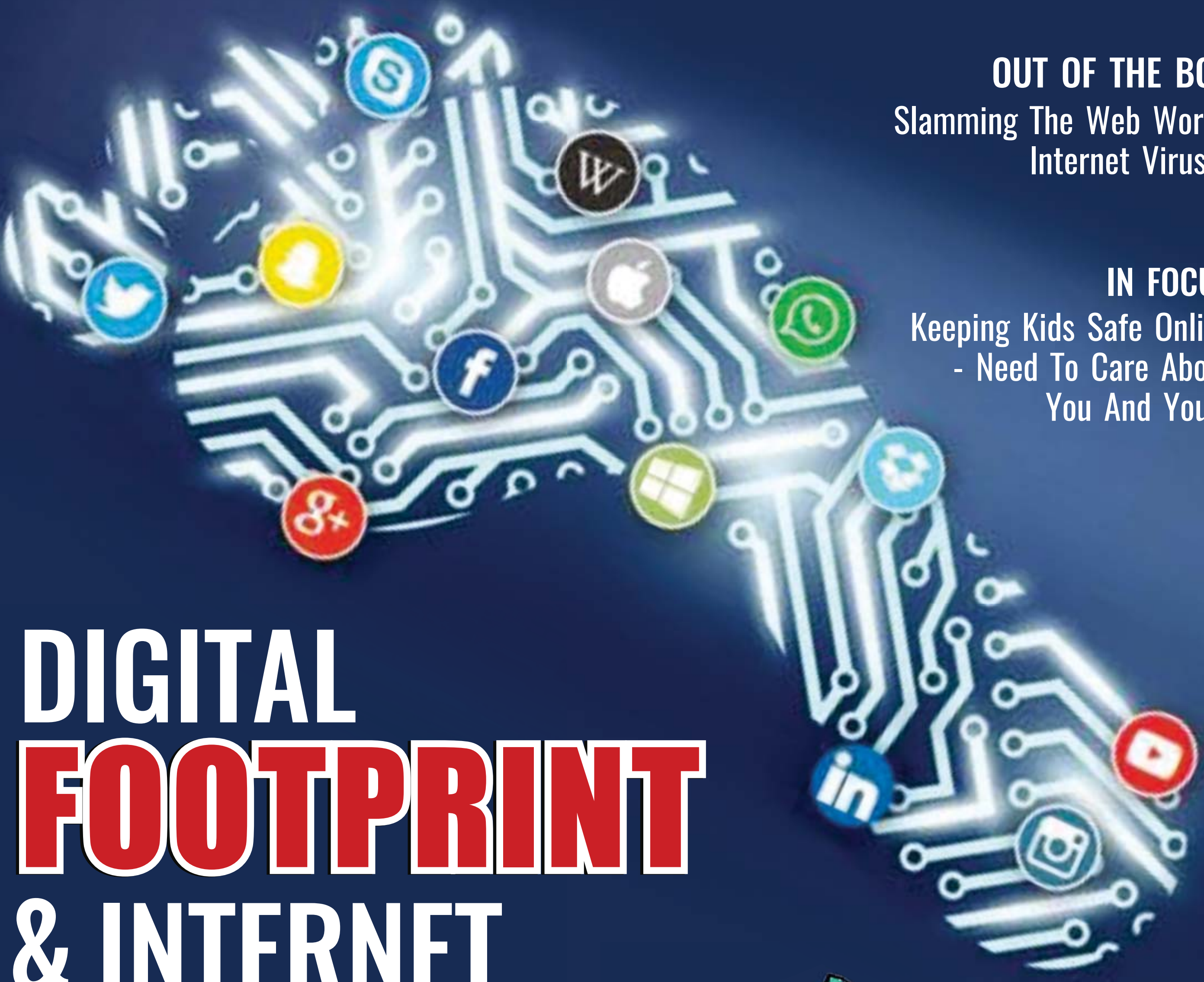
NOVEMBER 2018 • Vol. 4 • Issue 8
MONTHLY • Pages 64
₹ 200

RNI No.: DELENG/2015/67140; Published on: Every month; Posted at Lodi Road HPO, New Delhi on 9-10th of every month

THE AWARE CONSUMER

www.consumerconexion.org



OUT OF THE BOX

Slamming The Web Worm: Internet Viruses

IN FOCUS

Keeping Kids Safe Online - Need To Care About You And Yours

DIGITAL FOOTPRINT & INTERNET SAFETY

RESEARCH FEATURE

Think Before You Click

PLUS REPORT • MY MARKET • THE LAST MILE

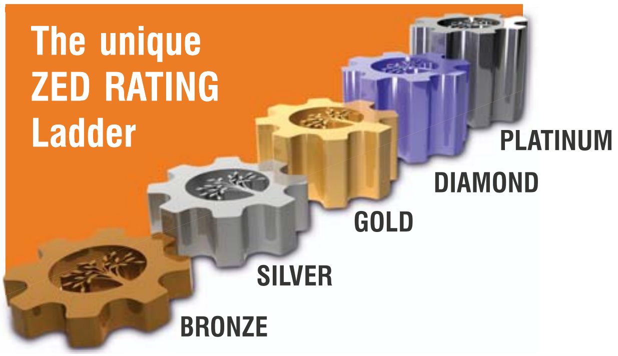
MAKE IN INDIA

QCI
Quality Council of India

ZED™
ZERO DEFECT • ZERO EFFECT

Certification Scheme

A roadmap to
World-class manufacturing



HIGHLIGHTS

- A scheme by Ministry of MSME, Govt. of India
- Certification on the systems and processes of MSMEs
- Handholding MSMEs towards world class manufacturing
- Special emphasis on MSMEs supplying to Defence Sector
- Direct subsidy to participating MSMEs
- Creating a credible database of MSMEs for OEMS/CPSUs/Foreign Investors under "Make in India initiative"
- Quality Council of India (QCI) to function as the NMIU (National Monitoring and Implementing Unit) of the scheme

> "Let's think about making our product which has 'Zero Defect'; so that it does not come back (get rejected) from the world market and 'Zero Effect' so that the manufacturing does not have an adverse effect on our environment"
>
> ***SHRI NARENDRA MODI***
> *Hon'ble Prime Minister*

**Free Registration at
www.zed.org.in**

zed@qcin.org   @ZED_QCI

VIEW POINT

BEJON KUMAR MISRA | bejonmisra@consumerconexion.org

Leave A Strong FOOTPRINT

WITH JUST A few hours of research online, it's possible to create a detailed profile of who you are, what you do and where you go? The same is true with organisations; as cybercriminals can, and regularly do build a detailed picture of their web assets, network touch-points and key employees in preparation for an attack. The technique they employ is called 'digital footprinting' and is a form of reconnaissance performed using relatively simple tools and techniques, together with the wealth of information freely available on the web. The latter is known as Open Source INTelligence (OSINT) in analyst circles.

Automated tools such as scanning engines provide cybercriminals with a convenient means of searching the web for organisations with weak security controls, and identifying potential misconfigurations and vulnerabilities.

In the retail sector for example, web applications and services such as those associated with storing card data and payment information, revenue generating web services, or management and integration of partner services make attractive targets.

Although digital footprints cannot be completely removed, there are ways to reduce the risk they pose. For individuals, this means being careful about the type of information they post online, and ensuring the privacy settings on their social networks and mobile phone applications are limited to known associates. For organisations, it means regularly scanning their external-facing infrastructure for potential vulnerabilities, ensuring they have full awareness and visibility of how they look from the outside, as well as conducting penetration testing and threat assessments.

Web authentication is headed for a sweeping change, as consumers and businesses increasingly look to a more effective way to establish identity and trust on the Internet. The spike in cyberattacks on consumers, private businesses and public bodies, has made people start to realize that the basic user-name-and-password form of security is not enough to protect oneself.

The way forward will be multifactor authentication. The world is moving beyond reactive security and toward context and identity-driven security models. It's not just much about keeping the bad guys out, but also letting the good guys in.

Perception is reality. With a strategy comprised of consistent content production and technology monitoring tools anyone can create a positive digital footprint and check for digital safety threats. The choice is yours as to whether or not you want your reality to be on the Internet. Don't roll the dice and let others dictate this for you.

> The spike in cyberattacks on consumers, private businesses and public bodies, has made people start to realize that the basic user-name-and-password form of security is not enough to protect oneself.

DESKTALK

Message from the Editor-in-Chief

POOJA KHAITAN
pooja@jagograhakjago.com

Right Foot Forward

IN THE AGE where billions of people have taken both their personal and professional lives online you better be cognizant of your digital footprint. With each Facebook post, email, Instagram photo, comment on a blog, YouTube video, Skype call, etc. you are leaving a trail that can be seen, searched, or tracked. Basically all of your activity on the Internet leads to the creation of a digital identity and footprint.

During the first decade of the 21st century, the internet was the site of what Miller (2011) has called 'a kind of social "big bang" leading to an expanded social universe' (2018). This increasingly ubiquitous embeddedness of social media in consumers' personal, working and learning lives brings certain pressures to bear: they need to know how to 'work' social media for their own professional and competitive advantage and also how to manage a 'digital footprint' that has the potential to deeply damage their employment opportunities and future personal wellbeing.

In some cases you might think that you have everything under control, right?

Wrong!

Your digital footprint is not only formed by what you post, but also what others put online about you.It can seem daunting to not only keep tabs on the digital footprint that you are actively crafting, but also on what other people are creating and posting at times unbeknownst to you.

The growth of the internet gave rise to many important services accessible to anyone with a connection. One of these important services is digital communication. While this service allowed communication with others through the internet, this also allowed the communication with malicious users. While malicious users often use the internet for personal gain, this may not be limited to financial/material gain. This is especially a concern to parents and children in particular, as children are often targets of these malicious users. Common threats to personal safety include: phishing, internet scams, malware, cyberstalking, cyberbullying, online preditions and sextortion.

Once we know what digital footprint is and the safety threats it attracts, it's time we take proper steps to cultivate and protect it. The digital world isn't going anywhere anytime soon—so think of it as a lifelong development. Take advantage of the platform to present yourself in a good and secure light and show off your best qualities. After all, you never know who will be looking in our newfound digital economy so it's best to put our right foot forward.

INSIDE

REGULARS

THE AWARE CONSUMER | NOVEMBER 2018

RESEARCH FEATURE

As we leave our digital footprint all over the web world, Internet safety or online safety is a must. Internet Safety is trying to be safe on the internet and is the knowledge of maximizing the user's personal safety and security risks to private information and property associated with using the internet, and the self-protection from computer crime in general.

HORIZONS

Most logins today are protected by a password. If an attacker can get your password, he can access your account and do anything you could do with that account. So when you ask how secure your account is, you're really asking how safe your password is.

GOVERNMENT PERSPECTIVE

AADHAAR serves as a Proof of Identity & Address, anywhere in India

THE AWARE CONSUMER
UNLOCKING CONSUMER POTENTIAL
www.consumerconexion.org

NOVEMBER 2018 • Vol. 4 • Issue 8

Bejon Kumar Misra
PUBLISHER
Address: F - 9, Second Floor, Kailash Colony,
New Delhi - 110048
E-mail: bejonmisra@consumerconexion.org

EDITOR-IN-CHIEF
Pooja Khaitan

EDITORIAL CONSULTANTS
Praful D. Sheth
Bina Jain
Suman Misra
Manisha Bhatla
Pyush Misra
Shashank D. Sudhi
Shashi Bhushan

MANAGER CIRCULATION
Nirmal Dayal

DESIGNER: Galaxy
DESIGN CONSULTANT: Maanav Khaitan

WEB DESIGNER:
Manish Mohan
Ebrahim Bhanpurawala

The AWARE CONSUMER
is printed and published by
Bejon Kumar Misra
at F - 9, Second Floor, Kailash Colony,
New Delhi - 110048 and printed at
M/s. Swastika Creation
19, D.S.I.D.C. Shed, Scheme 3,
Okhla Phase II,
New Delhi - 110020

Place of Publication: B - 306, First Floor,
C.R. Park, New Delhi-110019

For any queries, please contact us at
pooja@jagograhakjago.com
Phone: 011-26271421/22/23

Total number of pages - 64, Including Covers

DISCLAIMER: The views expressed in this magazine are solely those of the author in his/her private capacity and do not in any way represent the views of the Editor & Publisher.

Please Recycle This Magazine And Remove Inserts Before Recycling

RAKSHIT TANDON
DIRECTOR – A&R INFO SECURITY SOLUTIONS PVT. LTD.
CONSULTANT – INTERNET AND MOBILE ASSOCIATION OF INDIA.

Remain vigilant against the job frauds. Always check the senders e-mail address, grammatical mistakes in the mail, background of the hiring company and most importantly, never deposit any money.

ROUNDUP

BEING MEAN BEHIND THE SCREEN

WITH ACCESSING ONLINE information and interacting with data becoming a necessity rather than a habit, it has become very easy for thieves to steal your identity and personal information and use it for nefarious purposes. Your digital identity can be misused in a plethora of ways from opening a shady bank account, siphoning off your savings and making chargeable transactions to funding criminal networks. It, therefore, stands to reason that protecting the information that you share on public platforms is of paramount importance.

DATA BRIEFING

Internet penetration in India is around 8% (rising exponentially) with around 120 million Internet users.

How your personal information is tracked by websites

Most sites that let you access public information or put goods and services up for sale use bits of code, called cookies, to store your web browsing habits. They would typically capture details such as the time you spend on a site, a particular piece of content or product, how much time you spend looking at an advertisement, the sequence of clicks you make before buying an item, site preferences, return visits and so on. More intrusive sites will gather information that you share with social media platforms such as your age, gender, geographical location, the list of sites that you have bookmarked on your internet browser, the list of sites you have already visited in a single session and so on. Significantly, some sites will also save information such as your debit or credit card number, ostensibly for the purposes of saving you the effort of typing this data repeatedly every time you make a purchase. Other sites will attempt to bait you towards products that their sponsors are trying to sell by identifying patterns of online behaviour with known psychological profiles.

The perils of online activity

Marketing on the net has become considerably more subtle, with few organisations now directly engaging you on calls or flooding your message inbox with spam. Sellers do not make random target lists anymore. With the advent of internet mobility and smart devices measuring everything from your heart rate and blood pressure to your movements and bank balance, privacy would seem to have become obsolete. There is one more way in which

INSTAGRAM RELEASES PARENTAL GUIDELINES TO COUNTER CYBER BULLYING OF TEENS

DNA Web Team

With the number of individuals in their early teens joining social media giant Facebook's photo sharing service Instagram, there has been a need to ensure their safety. In May this year, Instagram unveiled an anti-bullying filter through which it would review accounts that have a large number of accounts filtered out. If those accounts violated the community guidelines, it would ban them. In addition, the new tool would hide comments and alert the company about repeat offenders.

While Instagram has been actively involved in curbing the meance of bullying through these tools, the damage on the victims at times can be irreversable, particularly at that age.

It is for this reason that Instagram conducted a workshop in Mumbai on 'Parents and Safety Measures on Instagram' where a guidebook for parents was released. nstagram published the guide last month in collaboration with ConnectSafely, a nonprofit organization “dedicated to educating users of connected technology about safety, privacy and security,” per its website.

The guide, if read, is more of an 'Instagram for Dummies', but gives us insights on things such as managing time on Instagram, a feature that this reporter was not aware of. It also provides a handy glossary and a list of questions parents can ask teens about their experiences.

"There are a number of tools that you can share with your teen to give them more control over their digital identity and footprint. One of the first things you will want to talk about with your teen is whether their account is going to be public or private. Making sure they understand that they have control over who sees and interacts with the things they post online will empower them to feel like they can be themselves on Instagram," Instagram has said in a blog.

Tara Bedi, Instagram's Public Policy & Community Outreach Manager, told DNA that while 13 is organisations are tracking and evaluating your behaviour. More and more employers are profiling your digital footprint with predictive models that tell them whether you will be a safe investment or not. Governments can trace your social media activity to decide whether you are for or against certain policy initiatives. More sinister is the fact that you can be manipulated based on tried and tested techniques to feed your hidden biases and engage your personal time with debates and activities that put a shadow on real issues that affect you.

There are frightening possibilities and parallels, here, with fiction from the 1930s and 1940s on the lines of Orwells '1984' or Huxley's 'Brave New World'. Statistically speaking, a large number of individuals can be controlled unconsciously by overarching systems to bring about an all-pervading perverse form of social engineering that upholds the position of those in authority and discourages or even punishes forms of behaviour it sees as disruptive to the status quo.

Pervasive and intrusive Social Media

Facebook is a well known social media platform that is known to be excessively intrusive. Its CEO, Mark Zuckerberg, was recently asked to present himself for questioning before the US Congress and the European Parliament. Zuckerberg inadvertently admitted that Facebook gathers extensive information about its users and also those who visit their platform without becoming subscribers themselves.

Democracy and the internet

While radio and TV have been subject to heavy regulation, the internet is still a minefield of unregulated activity. Even mobile apps entice you to give up personal information with the threat of you not being able to use its functionalities unless you share. The former may be an arena of debate with many users observing that the freedom of expression found on the internet is what makes it the last vestige of democratic articulation. But the more vivid your statements, the more notice you attract from the powers that be. Then there is the question of internet trolls backed by the latter who fully comprehend the power of anonymity and are yet another manifestation of the violence associated with anarchy. ◗

Making sure they understand that they have control over who sees and interacts with the things they post online will empower them to feel like they can be themselves on Instagram.

the legal age to get onto any Facebook-owned platform, there are parents who create accounts for their children and manage it until they reach a particular age. "This is usually seen in the case of celebrities, but there are regular people who also do this," she admits.

While warning of the dangers of bullying, she adds, "Let your teen know that if they spot an account, photo, video, comment, message or story that is intended to bully or harass someone, they can report it from within the app reporting the defaulter."

According to British anti-bullying organization Ditch The Label's new annual survey, Instagram is the network of choice for cyberbullies in 2017 with Facebook close behind. This year's survey collected results from 10,020 people between the ages of 12 and 20, which sheds some light into the damaging phenomenon endemic to internet communities, BGR India reported earlier this year.

Of these, 42% said they were bullied on Instagram. Of those who were bullied in the past one year, 37 percent developed social anxiety, 36 percent developed depression, and 24 percent had suicidal thoughts. 23 percent of these people even self-harmed, while 12 percent of them developed anti-social behaviour.

And while this guidebook for parents is just another step to curb online harassment, cyber bullying has a long way to go before it leaves our lives. ◗

Google, NCERT Partner To Bring Digital Citizenship And Safety Course To Classrooms

Google will partner NCERT, and enhance the ICT curriculum, to introduce a course on digital safety

(Image Source: Google)

Google has announced a collaboration with curriculum authority NCERT, which will introduce a Digital Citizenship and Safety course to the information and communications technology (ICT) curriculum.

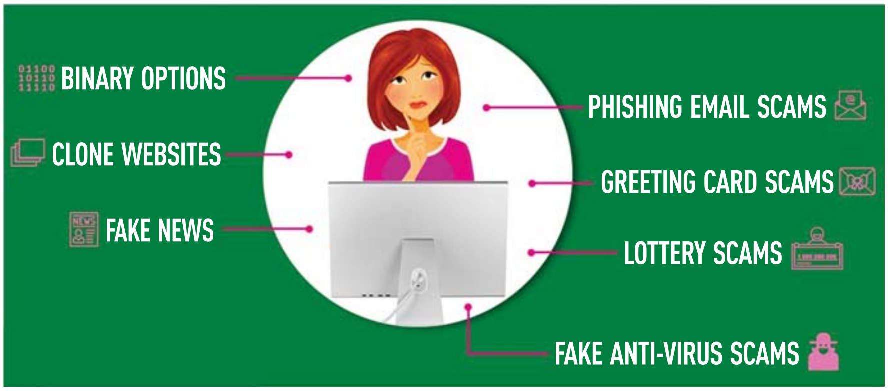
GOOGLE ANNOUNCED ITS partnership with NCERT on the Safer Internet Day 2018, to introduce a Digital Citizenship and Safety course in the ICT (information and communications technology) curriculum. The course has been designed to teach students the social, ethical and legal aspects of Internet safety. Google's Digital Citizenship and Safety coursework, evaluation has been divided in to four categories – Being Smart, Being Safe, Being a Digital Citizen and Being Future Ready. The course will also inform teachers about digital citizenship.

Divided across several levels, the course for lower classes will focus on engaging with technology and learning the use of basic digital tools. In middle classes students will be taught about the basics of the internet, concepts of account safety and distinguishing good content from bad. An advanced course includes topics such as privacy, device management, intellectual property and reputation management. Online financial literacy and cyber crime concepts will be introduced at graduation level of the course.

Consumers, Beware

Common Internet Scams

THE INTERNET IS a fertile breeding ground for deception and criminal scams. Here are some of the more prevalent culprits:

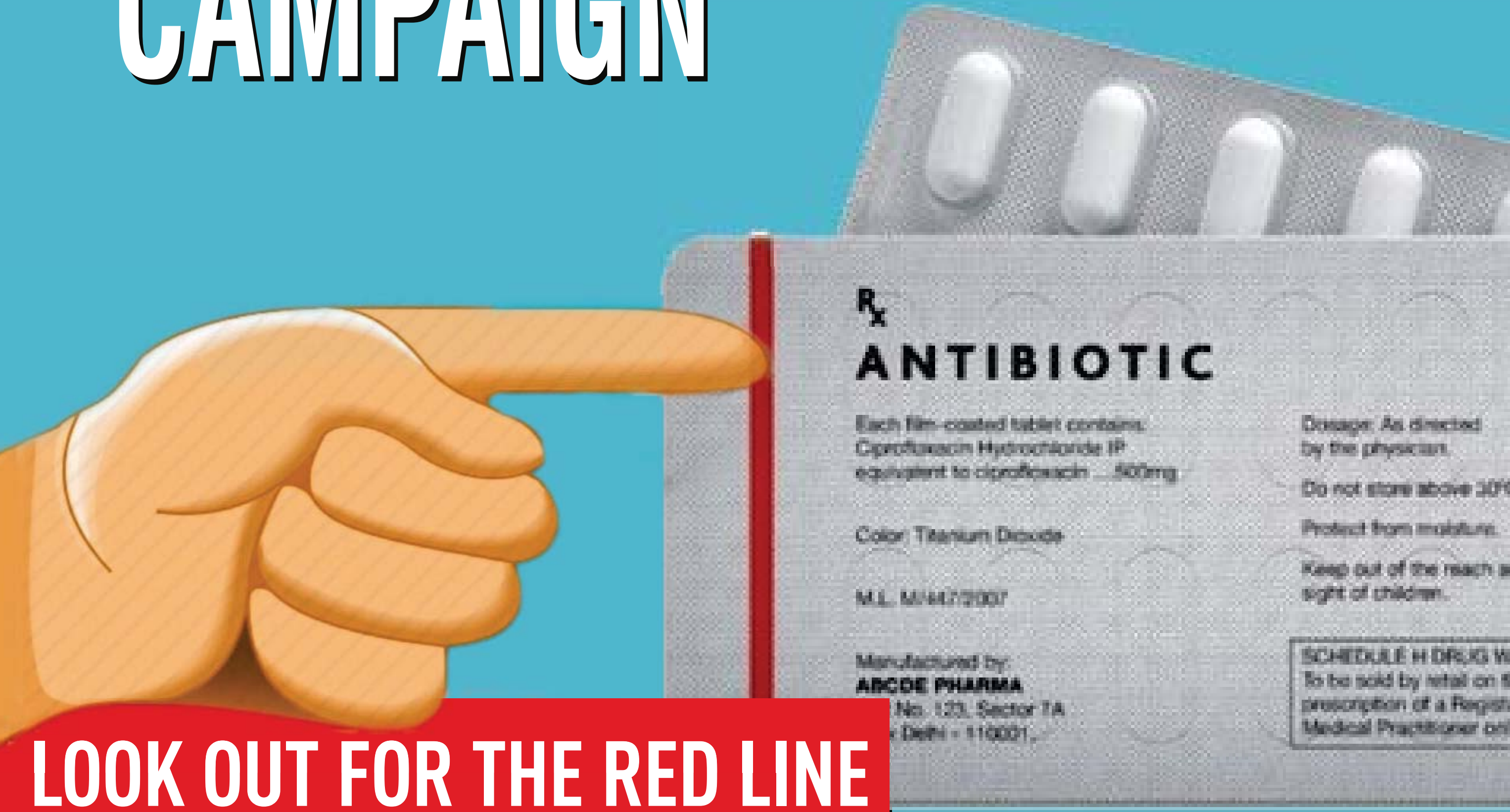


- The 'you've won the lottery' scam: An email arrives, informing you of your million-dollar lottery win. Of course, they'll need your full financial details so they can transfer these non-existent winnings into your account. Give them nothing and delete the email at once – without clicking on any links.
- The 'your account will soon be deactivated' scam: In this ploy, you get an email (allegedly from your bank or PayPal) saying there's a problem with your account, and you should click on a link to go to their site and correct the situation. Threats of account deactivation may persuade you into clicking on the link. Unfortunately, this link doesn't take you the genuine financial site – it takes you to a fake lookalike site that's aimed at getting sensitive information from you. Whenever you get one of these 'act immediately or your account will be frozen' emails, delete it at once. These emails rely on impulsive panic, but are easily thwarted by not clicking on links in emails from financial entities. When in doubt, call them on the phone.
- Lonely hearts scams: These scams often prey on older people, and can affect both sexes equally. A person worms their way into your online life and strikes up a friendship. The relationship deepens, and may turn to cyberspace romance. There may even be promises of marriage. Before long, they'll ask for a small 'loan' under some pretext: their child is sick, they need airfare money to come visit you, etc. If you pay, they'll thank you profusely, wait a suitable length of time, and ask for more money for something else – and on it goes. The person you've fallen for might not even exist: their photo could be a phony, and their life history a fairy tale.
- Nigerian inheritance scam: This one has become famous: you get an email from Prince Makatele Mubongo of Nigeria (or similar), telling of a massive inheritance that he desperately needs to get out of the country. Naturally, he has selected you to transfer this money to – provided you supply your banking details and pay an 'overseas bank transfer fee' of a few hundred dollars to get things rolling. If you send the money, you'll find there's been a glitch in the process, and even more money is required to smooth out the bureaucratic details. You'll never see a cent of this make-believe inheritance, but the make-believe Prince will do okay.
- The 'take our survey' scam: This is one of the most common ways for computer hackers to install malware or spyware on your computer. When you take the requested survey, these criminals install their programs and can then check on your every online move, scanning for passwords, credit card information and anything else usable for financial gain. Avoiding online surveys is a wise move. The survey may appear to be from a legitimate source (and may even promise a prize for participating), but a check of the sender's email address will usually reveal a suspicious URL. Delete it immediately.
- The 'work from home and make thousands a week' scam: The way these work is that you get an email (or respond to a pop-up on a site you've visited) telling you about the sure-fire way you can 'earn $5,000 a week while you sleep!' Upon responding, you'll discover that to get to the 'top earning level' you'll need to fork out for some training materials. If you don't, they'll typically bombard you with emails to ask why you haven't taken this 'simple step towards financial freedom'. A variation on this theme is the fake (but extremely lucrative) job offer that asks for an upfront fee to 'process your application'.

These scams constitute just a sampling of the ways unscrupulous folks might try to extract money from you online. There are many others, but you can avoid most of them with simple vigilance.

Beware of anything that seems too good to be true. Delete unsolicited emails, adjust your privacy settings and don't click on links you're not sure about – especially from His Majesty Prince Baron von Ripyuoffkwik from Nigeria.

SUPPORT THE CAMPAIGN



Rx
ANTIBIOTIC
Each film-coated tablet contains: Ciprofloxacin Hydrochloride IP equivalent to ciprofloxacin ...500mg
Color: Titanium Dioxide
Dosage: As directed by the physician.
Manufactured by:
ABCDE PHARMA
SCHEDULE H DRUG

LOOK OUT FOR THE RED LINE

BE RESPONSIBLE

Medicines such as Antibiotics have a Red Vertical Line on their pack to indicate that these should be consumed only on doctor's prescription. Always complete the full course as prescribed by the doctor.

Campaign Partners

PATIENT SAFETY AND ACCESS INITIATIVE OF INDIA FOUNDATION
a Partnership for Safe Medicines India Initiative

Consumer Online Foundation

Healthy You Foundation

Consumer Conexion

SIGN THE PLEDGE.

HTTP://WWW.CAUSES.COM/CAMPAIGNS/106670-RAISE-AWARENESS-FOR-SALE-USE-OF-ANTIBIOTICS-TO-COMBAT-AMR

Digital Footprint And Internet Safety

A DIGITAL FOOTPRINT is a trail of data you create while using the Internet. It includes the websites you visit, emails you send, and information you submit to online services.

A **"passive digital footprint"** is a data trail you unintentionally leave online. For example, when you visit a website, the web server may log your IP address, which identifies your Internet service provider and your approximate location. While your IP address may change and does not include any personal information, it is still considered part of your digital footprint. A more personal aspect of your passive digital footprint is your search history, which is saved by some search engines while you are logged in.

An **"active digital footprint"** includes data that you intentionally submit online. Sending an email contributes to your active digital footprint, since you expect the data be seen and/or saved by another person. The more email you send, the more your digital footprint grows. Since most people save their email online, the messages you send can easily remain online for several years or more.

Publishing a blog and posting social media updates are another popular ways to expand your digital footprint. Every tweet you post on Twitter, every status update you publish on Facebook, and every photo you share on Instagram contributes to your digital footprint. The more you spend time on social networking websites, the larger your digital footprint will be. Even "liking" a page or a Facebook post adds to your digital footprint, since the data is saved on Facebook's servers.

Everyone who uses the Internet has a digital footprint, so it is not something to be worried about. However, it is wise to consider what trail of data you are leaving behind. For example, remembering your digital footprint may prevent you from sending a scathing email, since the message might remain online forever. It may also lead you to be more discerning in what you publish on social media websites. While you can often delete content from social media sites, once digital data has been shared online, there is no guarantee you will ever be able to remove it from the Internet.

How Do We Leave Digital Footprints? This happens in many ways.

Here are some of them:

Websites And Online Shopping

Retailers and product review sites often leave cookies on your system which can track your movement from site-to-site, allowing targeted advertisements that can show you products you've been recently reading about or looking at online.

Social Media

All those +1s, Retweets, and Facebook comments (even private ones) leave a record. Make sure you know what the default privacy settings are for your social media accounts, and keep an eye on them. Sites often introduce new policies and settings that increase the visibility of your data. They may rely on you just clicking “OK” to whatever terms they are introducing, without reading them.

Mobile Phones, Tablets, or Laptops

Some websites will build a list of different devices you have used to visit those sites. While this can often be used as a way to help secure your account, it is important to understand the information being collected about your habits.

How to minimise your digital footprint

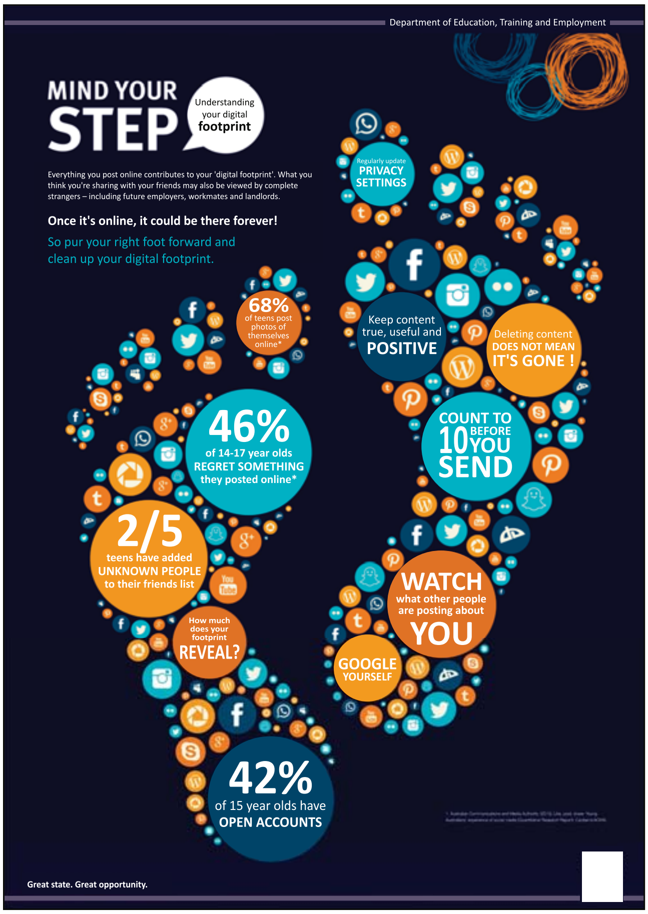
Make no mistake about it – the web is listening every time you use it! It's important that you understand what you're leaving behind when you visit a website.

An increasing number of young people are taking to the internet as a dint of habit. They rely on it to help them with their studies, news and random trivia and even to make friends. The ubiquity of cloud servers has meant that people upload their videos, images and personal documents without thinking about who or which entities can access this information. So, digital footprints left by them can be very wide. Fortunately, there are tools available that help you manage the quantity and type of information you share online. Digital information is often highly moldable. This means that the information that you share online can be tweaked.

Most users forget to use Privacy setting on their browser. It may be convenient but not practical to not delete cookies and browsing history after every session. You can use 'Ad blockers' to bar intrusive scripts. It will take some effort and engagement to check your Google privacy settings, Linkedin, Yahoo, Facebook and other email and social data settings to 'uncheck' the options that legally permit these portals to save your browsing habits. Take no heed of how much they dress up these activities with attractive words. Google will typically track every search and keywords you type in or speak at your microphone, especially if you're logged in. Googling yourself by name will tell you part of the results that are public information against your name. Use secondary emails to subscribe to intrusive platforms or apps. Never save passwords on your computer or smartphone. These are paltry measures compared to the number of ways in which your digital footprint is traced. But it's a step in the right direction to ensuring a safe, healthy and private future.

Managing your digital footprint:

- **Google yourself:** Take inventory of what's out there. Search for your name every few months, so you're cognizant of the information others have access to.



Department of Education, Training and Employment

MIND YOUR STEP

Understanding your digital footprint

Everything you post online contributes to your 'digital footprint'. What you think you're sharing with your friends may also be viewed by complete strangers – including future employers, workmates and landlords.

Once it's online, it could be there forever!

So pur your right foot forward and clean up your digital footprint.

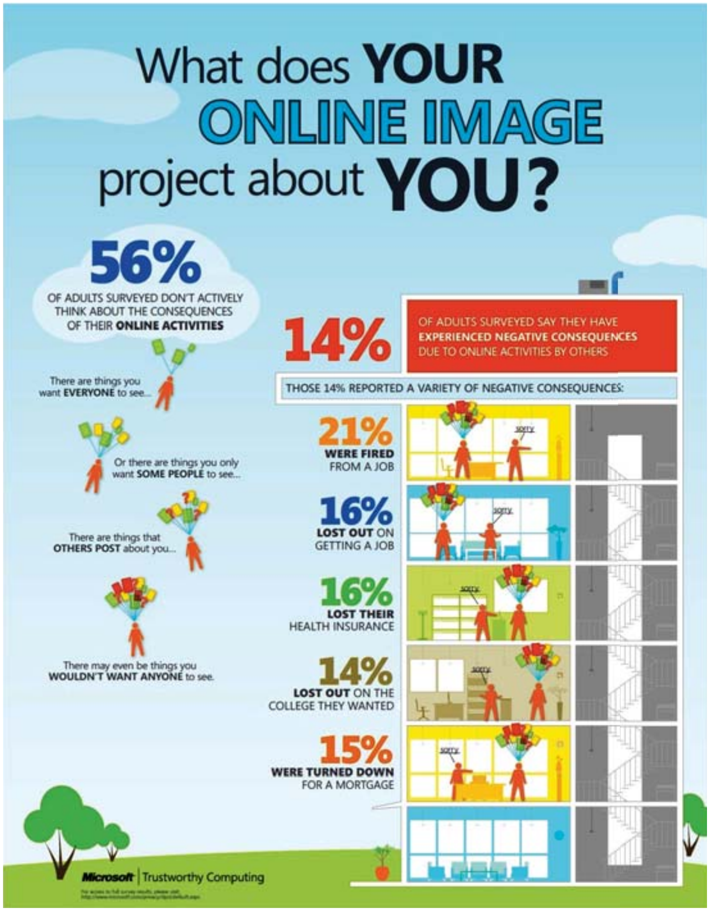
68% of teens post photos of themselves online*
46% of 14-17 year olds REGRET SOMETHING they posted online*
2/5 teens have added UNKNOWN PEOPLE to their friends list
How much does your footprint REVEAL?
42% of 15 year olds have OPEN ACCOUNTS
Regularly update PRIVACY SETTINGS
Keep content true, useful and POSITIVE
Deleting content DOES NOT MEAN IT'S GONE !
COUNT TO 10 BEFORE YOU SEND
WATCH what other people are posting about YOU
GOOGLE YOURSELF

Great state. Great opportunity.

- **Set up Google alert:** set up a Google alert for your name. The tool will then send you occasional alerts of every post that has your name on it.
- **Protect your personal data:** Don't disclose your personal address, phone number, passwords or bank card numbers. Consider using a nickname instead of your real name.
- **Keep login info under lock and key:** Never share any of your usernames or passwords with anyone.
- **Think before you post:** Never put a temporary emotion on the permanent internet. Anger is temporary; online lasts forever. Pause before you post: Think twice, post once.
- **Nix the pics:** Any photo you post could be dug up some day. Limit your sharing of questionable images. Fifteen minutes of humor is never worth a lifetime of potential humiliation.

Benefits of a digital footprint

When done wrong, your digital footprint can be detrimental, but it's not all doom and gloom. When they're done right, a digital footprint can provide you with a great first impression. You're now aware that employers



are following your trail, so take advantage of it. There are many ways you can leverage your digital skills to land a job.

A strong online presence, or digital footprint, can be a career asset in today's competitive job market. Many employers are performing online searches—in addition to reviewing resumes and cover letters—in an attempt to learn about prospective hires, including their interests, industry involvement and, more important, their ability to market themselves effectively.

If hiring managers are impressed by the content they find, like thought-provoking commentary or links to industry articles, they may be more apt to reach out to individuals for an interview. On the other hand, a lack of activity can be a turn-off.

With the digital economy now driving much of the workforce, reinforcing your technical prowess with a strong digital presence can be helpful to job seekers.

Your digital footprint is now a reality of life. If you want to do anything big in the world, you're going to have to understand how to craft your footprint and use it. Individuals control the narrative through personal branding—have a theme or style woven throughout your social media and website. This will make it easier for readers to tell what content is verifiably from you and what could have been put out by someone else about you.

COMMON THREATS TO PERSONAL DIGITAL SAFETY

As we leave our digital footprint all over the web world, Internet safety or online safety is a must. Internet Safety is trying to be safe on the internet and is the knowledge of maximizing the user's personal safety and security risks to private information and property associated with using the internet, and the self-protection from computer crime in general.

As the number of internet users continues to grow worldwide,internets, governments and organizations have expressed concerns about the safety of their citizens and children in particular using the Internet.

Common causes of information security breaches

Phishing

Phishing is a type of scam where the scammers disguise as a trustworthy source in attempt to obtain private information such as passwords, and credit card information, etc. through the internet. Phishing in unfortunately very easy to execute. It consists of fake emails or messages that look exactly like emails from legitimate companies. You are deluded into thinking it's the legitimate company and you may enter your personal and financial information.Phishing often occurs through emails and instant messaging and may contain links to websites that direct the user to enter their private information. These fake websites are often designed to look identical to their legitimate counterparts to avoid suspicion from the user.

Internet scams

Internet scams are schemes that deceive the user in various ways in attempt to take advantage of them. Internet scams often aim to cheat the victim of personal property directly rather than personal information through false promises, confidence tricks and more.

Malware

Malware, particularly spyware, is malicious software disguised as software designed to collect and transmit private information, such as passwords, without the user's consent or knowledge. They are often distributed through e-mail, software and files from unofficial locations. Malware is one of the most prevalent security concerns as often it is impossible to determine whether a file is infected, despite the source of the file.

Spyware / Trojan Horse

A Trojan Horse is a malicious program that looks like a legitimate software. While installed on your computer it runs automatically and will spy on your system, or delete your files.

ONLINE PREDATORS

Online Predators use social networks to gain information about their victims...

LIKES
DISLIKES
HOME
SCHOOL

82% Likes and dislikes.

65% Home and school.

Of kids who have received sexual solicitations online...

50% Posted personal information

45% Interacted with online strangers

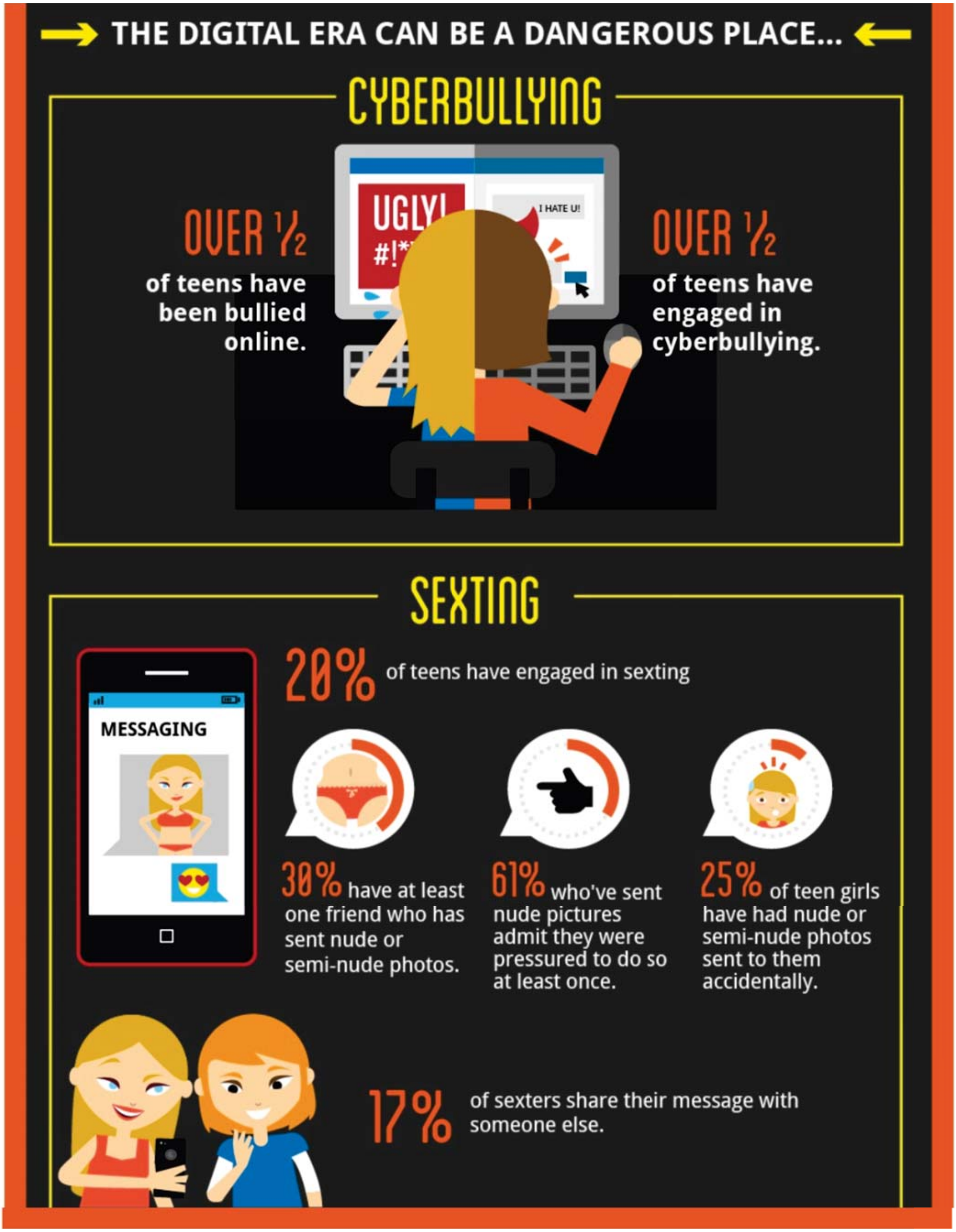
35% Placed strangers on their buddy lists

ACCESSING ADULT CONTENT

27% of children 10-17 have been exposed to unwanted sexual material.

Only 1 IN 3 young people view pornography intentionally.

Young people who look at violent X-rated material are 6 TIMES more likely to force others into sexual behavior.



THE DIGITAL ERA CAN BE A DANGEROUS PLACE...

CYBERBULLYING

OVER ½ of teens have been bullied online.

OVER ½ of teens have engaged in cyberbullying.

SEXTING

20% of teens have engaged in sexting

30% have at least one friend who has sent nude or semi-nude photos.

61% who've sent nude pictures admit they were pressured to do so at least once.

25% of teen girls have had nude or semi-nude photos sent to them accidentally.

17% of sexters share their message with someone else.

Computer worm

This is a very common security threat. A worm works on its own, lives in your computer, and propagates by sending itself to other computers.

Distributed denial-of-service attack

The attack strategy is to contact a specific website or server over and over again. It increases the volume of traffic and shuts down the website / server. The malicious user usually uses a network of zombie computers.

Pharming

Its objective is to convince you to visit a malicious and illegitimate website by redirecting the legitimate URL. You may then give your personal information to this malicious person.

Cyberstalking

[Cyberstalking] is the use of the Internet or other electronic means to stalk or harass an individual, a group of individuals, or an organization. It may include the making of false accusations or statements of fact (as in defamation), monitoring, making threats, identity theft, damage to data or equipment, the solicitation of minors for sex, or gathering information that may be used to harass. According to a study conducted by Baum et al. (2009), the rate of assault through electronic means such as e-mail or instant messaging was over one in four out of all stalking victims in the study.

Cyberbullying

Cyberbullying is the attack upon an individual or group through the use of electronic means such as instant messaging, social media, e-mail and other forms of online communication with the intent to abuse, intimidate, or overpower. In a 2012 study of over 11,925 students in the United States, it was indicated that 23% of adolescents reported being a victim of cyber bullying, 30% of which reported experiencing suicidal behavior.

Online predation

Online predation is the act of engaging an underage minor into inappropriate sexual relationships through the internet. Online predators may attempt to initiate and seduce minors into relationships through the use of chat rooms or internet forums. In a sample of 216 incarcerated sexual offenders, the behavior characteristics that emerged were categorized into three groups: A) manipulative - typically a child molester; B) Opportunist - typically a rapist and C) Coercive being a mixture of both rapists and child molesters.

Various websites on the internet contain material that some deem offensive, distasteful or explicit, which may often be not of the user's liking. Such websites may include internet, shock sites, hate speech or otherwise inflammatory content. Such content may manifest in many ways, such as pop-up ads and unsuspecting links.

> **Every tweet you post on Twitter, every status update you publish on Facebook, and every photo you share on Instagram contributes to your digital footprint.**

Sextortion

Sextortion, especially via the use of webcams, is a concern, especially for those who use webcams for flirting and cybersex. Often this involves a cybercriminalposing as someone else - such as an attractive person - initiating communication of a sexual nature with the victim. The victim is then persuaded to undress in front of a webcam, and may also be persuaded to engage in sexual behaviour. The video is recorded by the cybercriminal, who then reveals their true intent and demands money or other services (such as more explicit images of the victim, in cases of online predation), threatening to publicly release the video and send it to family members and friends of the victim if they do not comply. A video highlighting the dangers of sextortion has been released by the National Crime Agency in the UK to educate people, especially given the fact that blackmail of a sexual nature may cause humiliation to a sufficient extent to cause the victim to take their own life,in addition to other efforts to educate the public on the risks of sextortion.

The Internet has made our lives easier in many ways. We now shop online, keep in touch with friends, pay bills, market our businesses and keep up with current affairs in cyberspace.

The Internet is also incredibly useful for finding information that would have required a trip to the local library 30 years ago. Need to check out the 12th game of the 1927 world chess championship or find the best hotel in Santa Cruz, Bolivia? Want a quick recipe for pumpkin soup or a tutorial on video editing? You can get all this and more in a matter of minutes online.

Criminals are also excited about this wealth of information, because it gives them access to personal details that can be used for unlawful activities. Staying safe online is mostly about being alert to the dangers.

TIPS FOR INCREASING YOUR INTERNET SAFETY

DON'T BECOME A victim of identity theft. Thieves only need to collect a few pieces of information before they have enough to steal your identity.

Identity theft is a serious issue. Criminals increasingly turn to the Internet for easy pickings. In 1 out of 5 instances, your stolen identification details are used to gain credit or apply for a loan. Around a third of identity theft victims don't even realise anything has happened until they receive an official notification or query from a government agency or their bank.

Although people often use the terms interchangeably, there are distinct differences between identity theft and identity fraud.

IDENTITY THEFT: Identity theft occurs when a thief accesses your personal information in order to impersonate you (in person or online), mainly to open accounts in your name. They might even use your details to take control of your existing accounts.

IDENTITY FRAUD: Identity fraud is a little different. Instead of stealing your identity, the thief uses your details to create a fictitious person in order to defraud merchants.

Both identity theft and identity fraud are sinister crimes that affect all consumers, because merchants, credit card issuers, utility companies and other entities must factor these crimes into their pricing structure, resulting in higher costs for everyone.

Thieves only need to collect a few pieces of information before they have enough to steal your identity. They're after details like your full name (especially as it appears on your credit card), date and place of birth, email address, physical address (including previous residences), passport or driver's license numbers, credit card details (expiration date, PIN, card number and security code), where you do your banking, phone number, employment history, club memberships and even your hobbies.

- It's impossible to completely eliminate identity theft, but there are several steps you can take to reduce your risk of becoming a victim:
- Keep your smartphone, tablet and other portable devices safe – they may have as much personal information in them as your purse or wallet.
- Check your bank and superannuation statements regularly to check for unusual activity.
- Unless you know and trust the sender, never open links or attachments in an email. Type a known address into your browser instead. Clicking on a link may lead you to a bogus lookalike site designed to extract personal details.
- Cut down on the personal information you share on social media sites – these are a favourite hunting ground for identity thieves.
- Improve your passwords, and don't use the same password for everything.
- Check your credit history regularly.
- Don't do any online banking or make payments on public computers – use your PC at home instead.
- Only download apps from reputable sources. Viruses are easily transmitted to your devices through dodgy downloading sites.
- Change your browser settings to disable pop-ups. Pop-ups are commonly used by criminals to install spying or key-stroke detection programs onto your computer to access banking details, passwords and other information.
- Install quality, up-to-date anti-virus software on your PC and devices.

If you believe you have become a victim of identity theft, notify the police immediately as well as any financial institutions or businesses that might be affected.

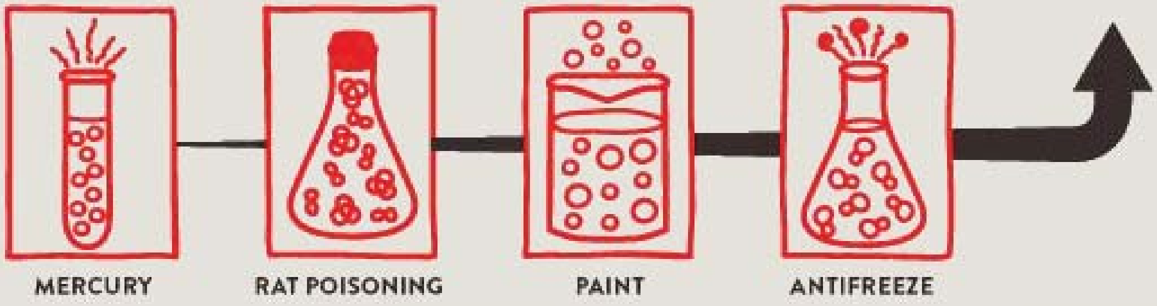
FIGHT THE FAKES

SPEAK UP ABOUT FAKE MEDICINES

VISIT FIGHTTHEFAKES.ORG

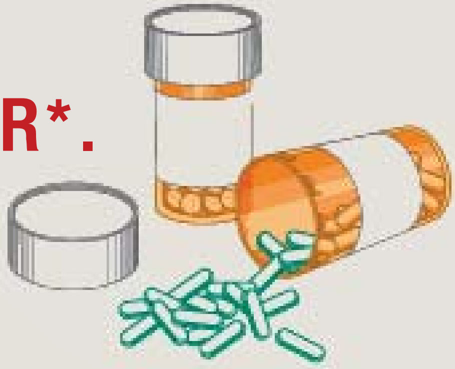
FAKE MEDICINES HARM – NOT HEAL

There are a lot of shady ingredients found in fake medicines that are directly responsible for serious disability and even death. This includes poisons such as mercury, rat poison, paint and antifreeze.



Fake tuberculosis and malaria drugs alone are estimated to

KILL 700,000 PEOPLE A YEAR*.



*International Policy Network

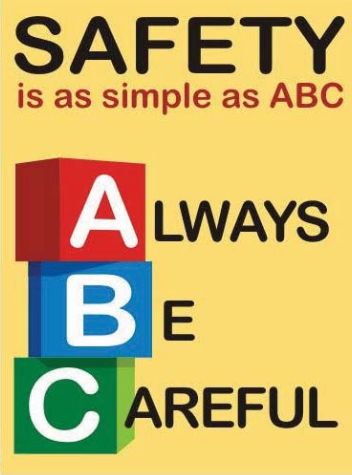
The Nature Of Personal Information Is Changing In The Age Of

Internet users are becoming more aware of their digital footprint; 47% have searched for information about themselves online, up from just 22% five years ago

THE VAST ARRAY of data points that make up "personal information" in the age of online media are nearly impossible to quantify or neatly define. Name, address, and phone number are just the basics in a world where voluntarily posting self-authored content such as text, photos, and video has become a cornerstone of engagement in the era of the participatory Web.

The more digital footprint we leave behind or the more content we contribute voluntarily to the public or semi-public corners of the Web, the more we are not only findable, but also knowable.

Internet users are becoming more aware of their digital footprint; 47% have searched for information about themselves online, up from just 22% five years ago



Unlike footprints left in the sand at the beach, our online data trails often stick around long after the tide has gone out. And as more internet users have become comfortable with the idea of authoring and posting content online, they have also become more aware of the information that remains connected to their name online.

Nearly half of all internet users (47%) have searched for information about themselves online, up from just 22%, as reported by the Pew Internet Project in 2002. Younger users (under the age of 50) are more prone to self-searching than those ages 50 and older. Men and women search for information about themselves in equal numbers, but those with higher levels of education and income are considerably more likely to monitor their online identities using a search engine.

Few monitor their online presence with great regularity

Just 3% of self-searchers report that they make a regular habit of it and 22% say they search using their name "every once in a while." Three-quarters of self-searchers (74%) have checked up on their digital footprints only once or twice.

Most internet users are not sure exactly what personal information is available online, however:

- Roughly one third of internet users say the following pieces of information are available online: their email address, home address, home phone number, or their employer. One quarter to one third of internet users say they do not know if those data points are available online.
- One quarter of internet users say a photo, names of groups they belong to, or things they have written that have their name on it appear online.
- Few internet users say their political affiliation, cell phone number, or videos of them appear online.

In interviews with the Pew Internet Project, privacy advocates and professional researchers argued that many of these data points are indeed available about most people, either on the open Web or in select online databases.

Most internet users are not concerned about the amount of information available about them online, and most do not take steps to limit that information.

Fully 60% of internet users say they are not worried about how much information is available about them online.

Similarly, the majority of online adults (61%) do not feel compelled to limit the amount of information that can be found about them online. Just 38% say they have taken steps to limit the amount of online information that is available about them.

Online adults can be divided into four categories based on their level of concern about their online information and whether or not they take steps to limit their online footprint:

- **Confident Creatives** are the smallest of the four groups, comprising 17% of online adults. They say they do not worry about the availability of their online data, and actively upload content, but still take steps to limit their personal information.
- The Concerned and Carefulfret about the personal information available about them online and take steps to proactively limit their own online data. One in five online adults (21%) fall into this category.
- Despite being anxious about how much information is available about them, members of the **Worried by the Wayside** group do not actively limit their online information. This group contains 18% of online adults.
- The **Unfazed and Inactive** group is the largest of the four groups—43% of online adults fall into this category. They neither worry about their personal information nor take steps to limit the amount of information that can be found out about them online.

Internet users have reason to be uncertain about the availability of personal data; 60% of those who search for their names actually find information about themselves online, but 38% say their searches come up short

The majority of internet users who have the inclination to query their names with a search engine do find some relevant results (60%), but a sizable segment (38%) report that a simple search does not yield any information connected to their name.

Among those who have searched for their name online, 62% find that the amount of relevant information about them generally matches their expectations. One in five self-searchers (21%) are surprised by how much information they find online about themselves, while 13%

express disbelief at how little information comes up in their results.

- Fully 87% of self-searchers who locate information connected to their name say that most of what they find is accurate, up significantly from the 74% who reported this five years ago.
- In contrast, 11% of self searchers who find information about themselves online say that most of it is not accurate, down from 19% five years ago.
- Just 4% of all online adults say they have had bad experiences because embarrassing or inaccurate information was posted about them online.

One in ten internet users have a job that requires them to self-promote or market their name online.

While most Americans do not actively manage their online presence, there is a segment of internet users who have jobs that require them to market their name on the internet or make information about themselves available online. As one might expect, those motivated by work-related expectations are much more likely to use a search engine to track their digital footprints.

- Those with the highest education levels report a greater tendency towards managing their professional presence online. Fully 18% of working college graduates report that their employer expects some form of self-marketing online as part of their job, compared with just 5% of working adults who have a high school diploma.
- Employees who are required to market themselves online are far more likely to monitor their presence with a search engine. Fully 68% of these “public personae” use a search engine to look up their own name, compared with just 48% of employed internet users who are not required to market themselves online as part of their job.
- One in five working American adults (20%) says their employer has a special policy about how employees present themselves online—including what can be shared and posted on blogs and other websites.

Among adults who create social networking profiles, transparency is the norm.

The Pew Internet Project has reported extensively on teenagers' use of social networking websites, finding that 55% of online teens have created an online profile and that most restrict access to them in some way. Looking at adults, their use of social networking profiles is much lower (just 20%), but those who use the sites appear to do so in a more transparent way.

- Among adult internet users who maintain an online profile, 82% say that their profile is currently visible compared with 77% of online teens who report this.
- Among adults who say they have a visible profile, 60% say that profile can be seen by anyone who happens upon it, while 38% say their profile is only accessible to friends.
- Teens with visible profiles make more conservative choices with respect to visibility; just 40% said their profile was visible to anyone, while 59% reported access that was restricted to friends only.

More than half of all adult internet users have used a search engine to follow others' footprints.

When asked about eight different groups of people one might search for online—ranging from family and friends to romantic interests and business colleagues—53% of adult internet users said they had looked for information connected to at least one of these groups.

- Most are casually curious in their searches for others. Just 7% of those who have searched for information on key people in their lives report doing so on a regular basis.
- Users are most likely to search for someone they have lost touch with. Fully 36% of adult internet users say they have used a search engine to find information about someone from their past.
- 19% of adult internet users have searched for information about co-workers, professional colleagues or business competitors.
- 11% of adult internet users say they have searched online for information about someone they are thinking about hiring or working with.
- 9% of online adults say they have searched online for information about someone they are dating or in a relationship with. Perhaps due to safety concerns, online women tend to do their dating homework more than online men.

Basic contact information tops most searchers' wish lists.

Despite all the new forms of personal information available online, the most popular type of “people search” relates to finding someone's contact information, like an address or phone number.

- 72% of people searchers have sought contact information online.
- 37% of people searchers look to the Web for information about someone's professional accomplishments or interests.
- 33% of people searchers have sought out someone's profile on a social and professional networking site.
- 31% have searched for someone's photo.
- 31% have searched for someone else's public records, such as real estate transactions, divorce proceedings, bankruptcies, or other legal actions.
- 28% have searched for someone's personal background information.

PASSWORDS:
Layer Up Your Login

Most logins today are protected by a password. If an attacker can get your password, he can access your account and do anything you could do with that account. So when you ask how secure your account is, you're really asking how safe your password is.

PASSWORD SECURITY IS one of the most commonly ignored aspects of online safety. If someone discovers your passwords, they have immediate access to all your personal online information – including your financial details.

More and more of the sensitive, valuable things in our life are guarded through password-protected online accounts — love letters, medical records, bank accounts and more. Web sites use login procedures to protect those valuable things. As long as someone can't log into your account, they can't read your email or transfer money out of your bank account. As we live our lives online, how should we protect our logins?

Ideally, you should never write passwords down. If you do, don't store them anywhere near your computer. Don't hide your password under your mouse pad or keyboard, on a note taped to the underside of your desk, under your landline phone or in the top drawer of your desk. Leaving your password in a 'clever' spot near your computer is a bit like leaving your front door house key under the mat, on top of the doorsill or wedged under a potted plant: thieves know all about these obvious hiding places.

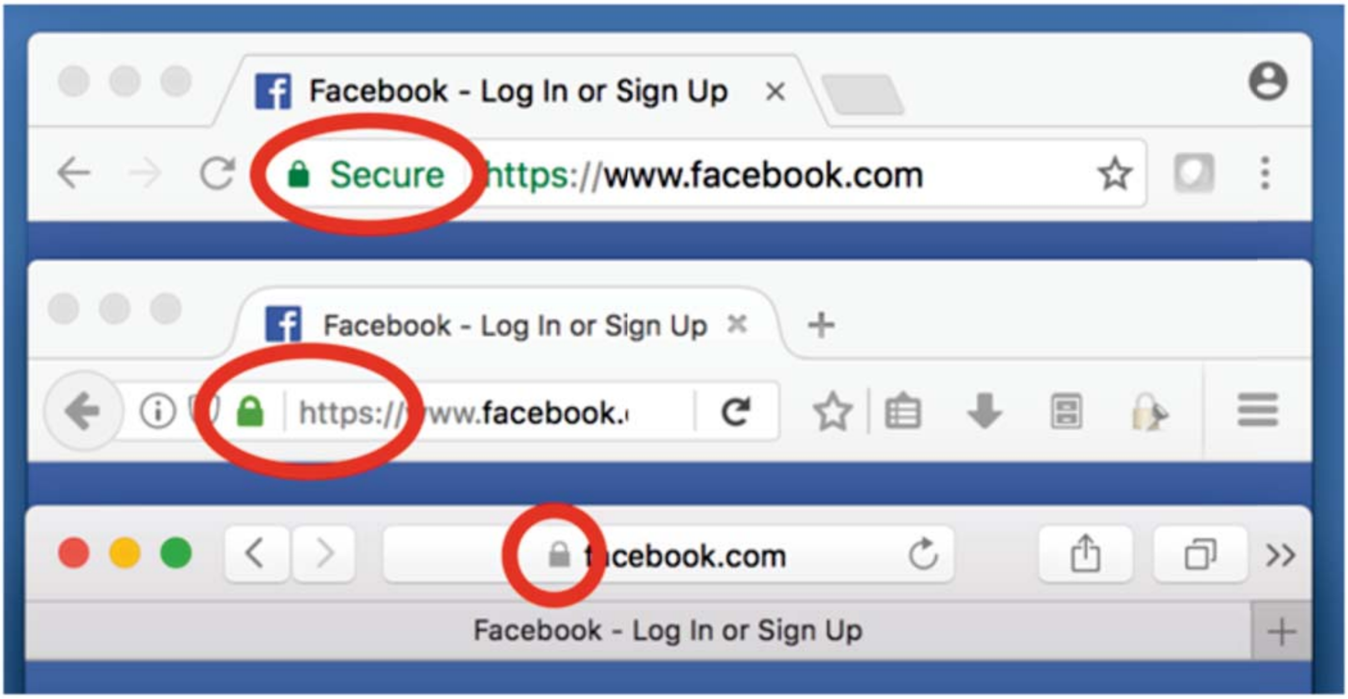
Passwords should be a random collection of letters (in both upper and lower case), numbers and symbols. Avoid choices that are easy to guess (like 123456 or the word 'password'), and change your passwords regularly.

A longer password is more secure than a short one.

Don't use the same password for everything – this makes it much too easy for criminals.

If keeping track of all your passwords becomes too much, there are a number of password management systems (some free, some not) that can assist you.

Usernames and passwords are simply not enough to secure online accounts. Millions of people have had their digital accounts hacked because of stolen credentials or weak logins, but many are not using widely available, simple technologies to better secure their online accounts. The best way to empower individuals to better protect their online accounts is by adding a layer to their passwords. Every person active on the web should bolster their online accounts by enabling the strongest authentication tools available so everyone can enjoy greater peace of mind knowing their online accounts are more secure. Intel recommends adding protective layers- sometimes called multi-factor authentication to passwords. Simply adding the requirement of a fingerprint or other secure factor to your login provides powerful protection - even in cases where current passwords are leaked or stolen. The combination of using a physical component like your smart phone together with the strong unique password you have for each


Facebook - Log In or Sign Up
Secure
https://www.facebook.com
Facebook - Log In or Sign Up
https://www.facebook.
facebook.com
Facebook - Log In or Sign Up

account, preferably stored in your password manager, takes security up a notch!

The different ways that an attacker could access your account's password:

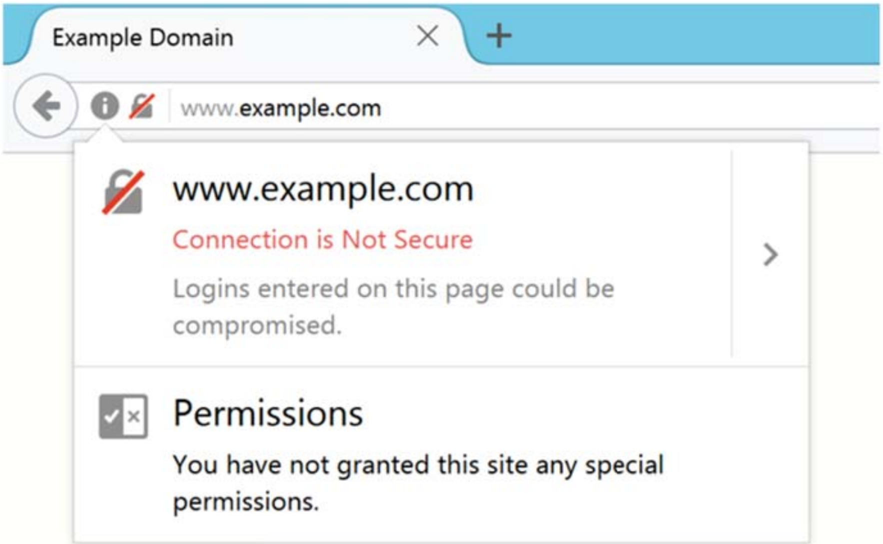
- Seeing you use it with an unencrypted website
- Guessing it
- Stealing a file that has your password in it
- Using password recovery to reset it
- Tricking you into giving it to them

To keep your login safe, you need to prevent as many of these as possible. Each risk has a different corresponding mitigation.

Look for the lock

It's easy to prevent attackers from stealing your password when you log into an unencrypted website: Never type your password unless you see a lock icon in the URL bar, like this:

The lock means that the website you're using is encrypted, so that even if someone is watching your browsing on the network (like another person on a public WiFi hotspot), they won't be able to see your password. Browsers are starting to roll out features that warn you when you're about to enter your password on an unencrypted site.



www.example.com

Connection is Not Secure

Logins entered on this page could be compromised.

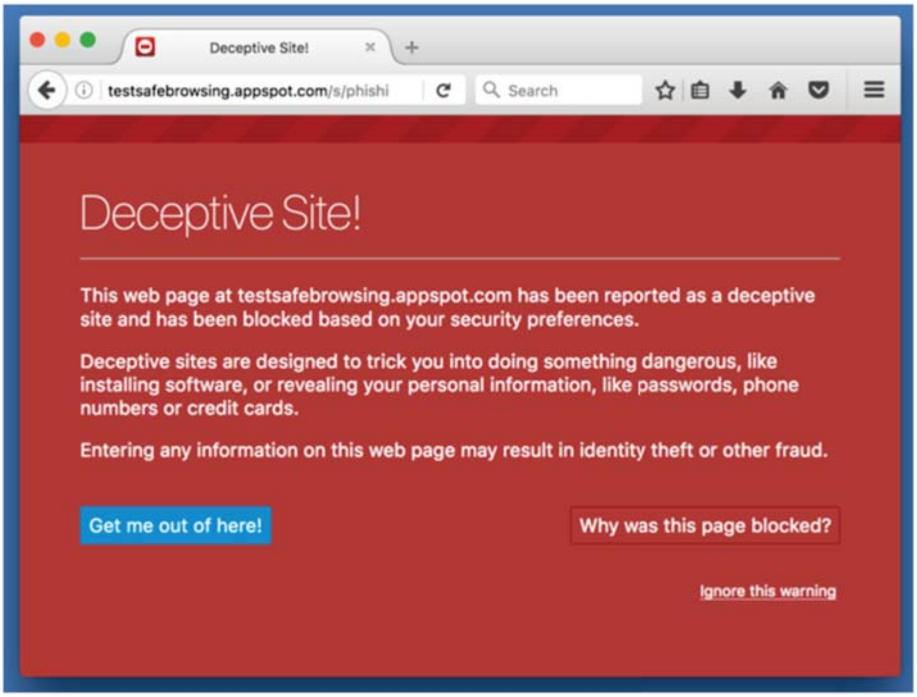
Permissions

You have not granted this site any special permissions.

Your browser also helps keep you informed about how trustworthy sites are, to help keep you safe from phishing. On the one hand, when you try to visit a website that is known to be a phishing site, any major browser will display a full-screen warning — **pay attention and don't use that site!**

On the other hand, when you're talking to a site that has provided proof of its legal identity, the browser will show you that identity. So for example, when you go to download Firefox, you can know that you're getting it from Mozilla.

In general, the best defense against phishing is to **be suspicious of what you receive,** whether it shows up in email, a text message or on the phone. Instead of taking action on what someone sent you, visit the site directly. If an email says you need to reset your Paypal password, don't click the link. Type in paypal.com yourself. If the bank calls, call them back.



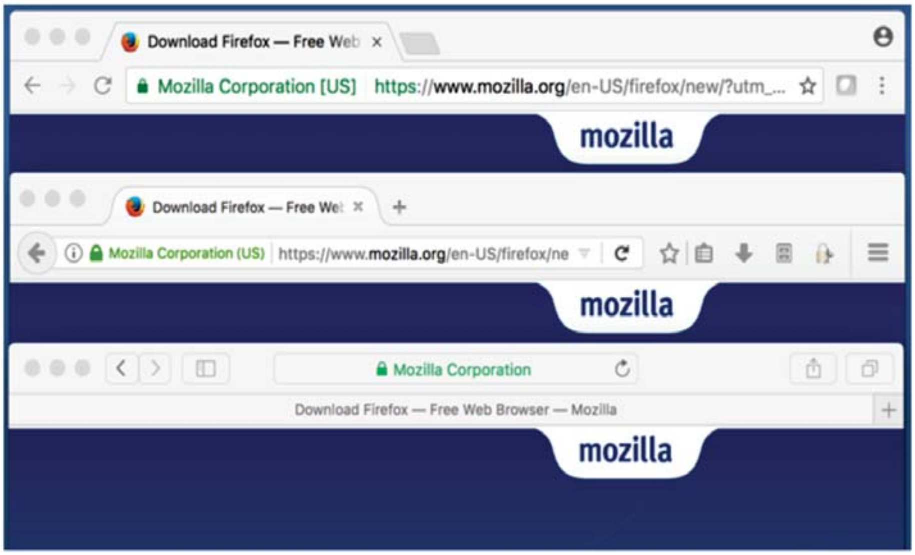
Deceptive Site!

This web page at testsafebrowsing.appspot.com has been reported as a deceptive site and has been blocked based on your security preferences.

Deceptive sites are designed to trick you into doing something dangerous, like installing software, or revealing your personal information, like passwords, phone numbers or credit cards.

Entering any information on this web page may result in identity theft or other fraud.

Get me out of here!
Why was this page blocked?
Ignore this warning


Download Firefox — Free Web
Mozilla Corporation [US]
https://www.mozilla.org/en-US/firefox/new/?utm_...
mozilla
Download Firefox — Free Web
Mozilla Corporation (US)
https://www.mozilla.org/en-US/firefox/ne
mozilla
Mozilla Corporation
Download Firefox — Free Web Browser — Mozilla
mozilla

Strength in diversity

The secret to preventing guessing, theft or password reset is a whole lot of randomness. When attackers try to guess passwords, they usually do two things: 1) Use "dictionaries" — lists of common passwords that people use all the time, and 2) make some random guesses. **The longer and more random your password is,** the less likely that either of these guessing techniques will find it.

When an attacker steals the password database for a site that you use (like LinkedIn or Yahoo), there's nothing you can do but change your password for that site. That's bad, but the damage can be much worse if you've re-used that password with other websites — then the attacker can access your accounts on those sites as well. To keep the damage contained, always use different passwords for different websites. There are also siteswhere you can subscribe to be notified if your account is in one of the password databases that has been stolen.

My mother's maiden name is "Ff926AKa9j6Q"

Finally, most websites have a password recovery system that lets you recover your password if you've forgotten it. Usually these systems make you answer some "security questions" before you can reset your password. **The answers to these questions need to be just as secret as your password.** Otherwise, an attacker can guess the answers and set your password to something he knows.

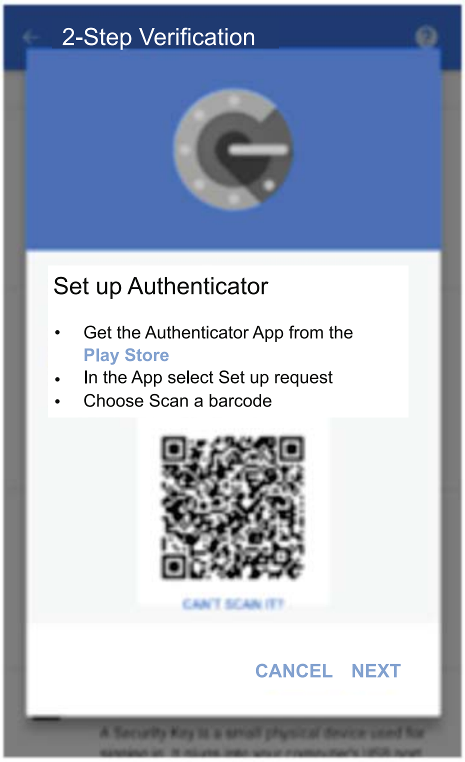
Randomness can be a problem, since the security questions that sites often use are also things people tend to know about you, like your birthplace, your birthday, or your relatives' names, or that can be gleaned from sources such as social media. The good news is that the website doesn't care whether the answer is real or not — you can lie! But lie productively: **Give answers to the security questions that are long and random,** like your passwords.

Get help from a password manager

Now, all of this sounds pretty intimidating. The human mind isn't good at coming up with long sequences of random letters, let alone remembering them. **You can use a password manager like 1Password, LastPass, or Dashlane to help improve your password hygiene.** They will generate strong passwords for you, remember them for you, and fill them into websites so you don't have type them in.

You do take on some risk by using one of these password managers,

Going old school.

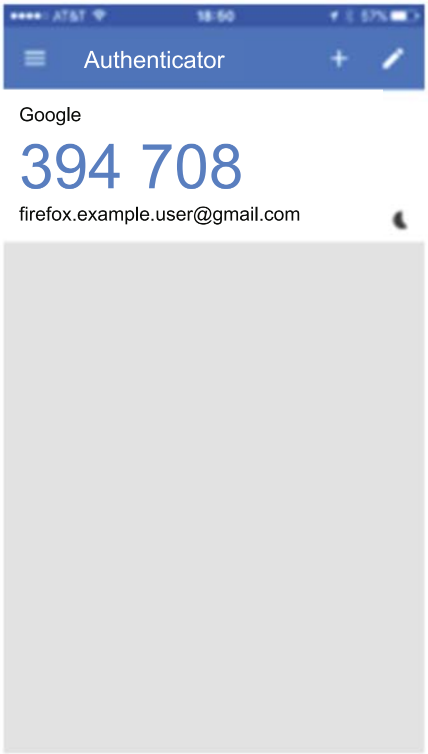


2-Step Verification

Set up Authenticator

- Get the Authenticator App from the Play Store
- In the App select Set up request
- Choose Scan a barcode

Set up a two factor authentication app.

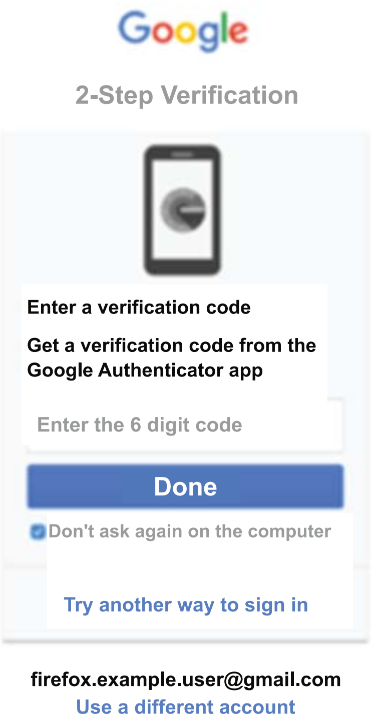


Google

394 708

firefox.example.user@gmail.com

Step 1. Generate authentication codes when you want to login.



2-Step Verification

Enter a verification code

Get a verification code from the Google Authenticator app

Enter the 6 digit code

☑ Don't ask again on the computer

firefox.example.user@gmail.com

Step 2. Enter the verification code to proceed with login.

since they create a database that has all your passwords in it. However, all reputable password managers encrypt their databases with a “master password.” The master password is safer from theft than normal passwords: Because it never gets sent to a server (just used on your computer to encrypt the database), an attacker has to break into your computer in particular, rather than a server where he can harvest millions of accounts. And because you only have to remember one master password, you can make it extra strong. So in general, it's much more likely that you'll have an account breached due to not using a password manager (e.g., a weak or re-used password) than that someone will both steal the your password manager's database and guess the master password.

Even if you can't figure out how to use a password manager, sometimes the simplest, least glamorous technology is also pretty secure: Just keep your written passwords in a safe place!

More factors, fewer problems

The other major step you can take to protect your account is to **add a “second factor” to the login process.** In most cases, the second factor is tied to your phone, which means that even if an attacker has your password, they can't log in to your account unless they also have your phone. (And vice versa — if your phone gets stolen, they can't log in unless they get your password.)

In order to enable two-factor authentication (or “2FA”), you'll need to associate your phone with your account on the website. Each website will provide instructions, but it usually involves either entering your phone number or scanning a barcode with a special app. Then, when you go to log in, the website will ask you for a code from your phone. If an attacker doesn't have your phone, he can't get the code, so he can't log in.

2FA provides much better security than passwords alone, but not every website supports it.

Strong, diverse, and multi-factor

For better or worse, we're going to be using passwords to protect our online accounts for the foreseeable future. Use passwords that are **strong** and **different for each site,** and use a **password manager** to help. Set **long, random answers** for security questions (even if they're not the truth). And use **two-factor authentication** on any site that supports it.

Following these steps takes some discipline and will make it harder to log in sometimes. But in today's Internet, where thousands of passwords are stolen every day and accounts are traded on the black market, it's worth some inconvenience to keep your online life safe. ◗

India's Biggest Digital Trick Or Treat?

How Safe Is Aadhaar Data?

With millions leaving their digital footprint in the web world, India is no exception. Bringing all personal information of citizens under one roof is the Aadhaar Card. How safe is the Aadhaar Data? Used and accepted on all digital platforms, the Aadhaar is secure and nothing can impact the security of Aadhaar database. This has been repeatedly affirmed by the Unique Identification Authority of India (UIDAI) in a series of tweets posted on its official handle-uidai.gov.in. According to UIDAI, the entire Aadhaar system is secure. This clarification came after rumours were surfaced on social media that Aadhaar PDF has been available on Google search. Aadhaar number is a 12-digit random number issued by UIDAI to the residents of India after satisfying the verification process, mentioned UIDAI on its official website-uidai.gov.in. Government made it mandatory to link Aadhaar with various services. However, the Supreme Court recently indefinitely extended the deadline to link phone, passport and bank accounts with Aadhaar number. Addressing the concern on data privacy, the latest ruling makes linking of the identification card with private services illegal. This also marks an end to any confusion regarding the services for which Aadhaar is mandated.

Here are 10 things to know about the security of Aadhaar system as mentioned on UIDAI's twitter handle:

1. Do not get carried away or confused with some news appearing in social and other media on Aadhaar pdf being available on Google search on Mera Aadhaar, Meri Pehchan.
2. UIDAI further said that such news are intended to spread misinformation on India's robust identity system - Aadhaar and are intentional and irresponsible acts of some unscrupulous elements.
3. These are far from the reality and have got nothing to do with the security of Aadhaar and its database. As none of the Aadhaar cards shown are taken from UIDAI database.
4. People share their personal information including Aadhaar on internet to some or other service provider or vendor to get the services and when they put their details on internet they should take due precautions as required in any digital activities.
5. Publications or posting of Aadhaar cards by some unscrupulous people have absolutely no bearing on UIDAI and not the least on Aadhaar security. Aadhaar as an identity document by its very nature needs to be shared openly with others as and when required.
6. Aadhaar is just like any other id, therefore, is never to be treated as a confidential document. By simply knowing someone's Aadhaar, no one can impersonate and harm him because Aadhaar alone is not sufficient, it requires biometrics to authenticate one's Identity.
7. Although Aadhaar has to be shared with others, it being personal information like mobile number, bank account number, PAN card, passport, family details, etc, should be ordinarily protected to ensure privacy of the person.
8. If anybody unauthorisedly publishes someone's personal information such as Aadhaar card, mobile number, bank account, photograph, etc., he can be sued for civil damages by the person whose privacy right is infringed.
9. However, in no way such publication threatens or impacts security of Aadhaar and its database. Aadhaar remains safe and secure and there has not been a single breach from its biometric database during that last eight years of its existence.
10. Aadhaar is the most trusted and widely held ID that one shows/presents whenever needed. People should freely use it to prove their identity.

Restricting Misuse Of Aadhaar Data - UIDAI

After a report exposed how access to the Aadhaar database could be bought on the internet only for Rs 500, a lot of concerns were expressed over the security of private data of citizens on the government portal. The Unique Identification Authority of India (UIDAI) had clarified that it was just a case of unauthorised access to the Aadhaar website and no biometric data was stolen. The incident led to a big debate over the security of Aadhaar database. There were a number of unanswered questions that created a lot of confusion among the people.

UIDAI has issued detailed FAQs on the safety and security of the Aadhaar database. Below are the answers to all your doubts about Aadhaar:

UIDAI has all my data including biometrics, bank account, PAN, etc. Will they be used to track my activities?

Absolutely false. UIDAI database has only the following information -

(a) Your name, address, DOB, gender, date of birth

In order to provide more choice to citizens authenticating using Aadhaar, the UIDAI has introduced face authentication along with fingerprints and iris.

(b) Ten finger prints, two IRIS scans, facial photograph

(c) mobile number and email ID .

Rest assured, UIDAI does not have your information about family, caste, religion, education, bank accounts, shares, mutual funds, financial and property details, health records etc and will never have these information in its database. In fact, Section 32(3) of the Aadhaar Act 2016 specifically prohibits UIDAI from controlling, collecting, keeping or maintaining any information about the purpose of authentication either by itself or through any entity.

AADHAAR serves as a Proof of Identity
& Address, anywhere in India

But when I link my bank accounts, shares, mutual funds and my mobile phones with Aadhaar, will UIDAI not get these information?

Absolutely No. When you give Aadhaar number to your banks, mutual fund companies, mobile phone companies, they only send Aadhaar number, your biometrics (given at the time authentication) and your name etc to UIDAI for verification for your identity. They do not send your bank account or its details to UIDAI. So far as UIDAI is concerned, it responds to such verification requests by replying either 'Yes' or 'No'. In few cases, if the verification answer is 'Yes', your basic KYC details (name, address, photo etc) available with UIDAI are sent to the service provider.

If someone gets to know my Aadhaar number, they can use it to hack my bank account.

Absolutely false. Just like by merely knowing your ATM card number, no one can withdraw money from the ATM machine, by knowing your Aadhaar number alone, no one can hack into your bank account and withdraw money. Your bank account is safe if you don't part with your PIN/OTP given by banks. Rest assured, there has not been a single case of financial loss due to Aadhaar.

Why am I being asked to link all my bank accounts with Aadhaar?

For your own security, it is necessary to verify identity of all bank account holders and link them with Aadhaar to weed out the accounts being operated by fraudsters, money-launderers, criminals etc. When every bank account is verified and linked with Aadhaar and then If anyone fraudulently withdraws money from your account, through Aadhaar such fraudster can easily be located and punished. Therefore, by linking your bank accounts with Aadhaar, your accounts becomes more secure and not the other way around.

Why am I being asked to verify and link my mobile numbers with Aadhaar?

For your own security and security of our country, it is necessary to verify identity of all mobile subscribers and link them with Aadhaar to weed out mobile numbers being operated by fraudsters, money-launderers, criminals etc. It has been found that most criminals and terrorists get SIM cards issued in the name of fictitious and even real people without their knowledge and use them for committing frauds and crime. When every mobile number is verified and linked with Aadhaar, then fraudsters, criminals, and terrorists using mobiles can be easily identified and punished in accordance with law.

Can the mobile company store my biometrics taken at the time of SIM verification and use it for other purposes later?

No one, including, mobile phone companies can store or use your biometrics taken at the time of Aadhaar verification and linking. The biometrics are encrypted as soon as Aadhaar holder places his finger on fingerprint sensor and this encrypted data is sent to UIDAI for verification. Regulation 17(1)(a) of the Aadhaar (Authentication) Regulations 2016, strictly prohibits any requesting entity which includes mobile phone companies, banks etc from storing, sharing or publishing the finger-prints for any reason whatsoever and neither shall it retain any copy of such fingerprints. Any violation of this provision is a punishable offence under the Aadhaar Act 2016.

How has Aadhaar benefited the common man?

Aadhaar has empowered 119 crore Indians with a credible identity. Today the fact is that Aadhaar inspires more confidence and trust than any other identity document in India. For example, if you are an employer, which identity document will you prefer from your prospective employees? Or, just ask your maid servant, household help, driver, poor living in slums and villages as to how they are using Aadhaar to prove their identity to get jobs, open bank accounts, for rail travel, and to get various entitlements and government benefits directly into their bank accounts without middlemen. Ask them and they will tell you how empowered they are by having Aadhaar.

We keep hearing in media that Aadhaar data was breached. Is it true?

Aadhaar database has never been breached during the last 7 years of its existence. Data of all Aadhaar holders is safe and secure. Stories around Aadhaar data breach are mostly cases of mis-reporting. UIDAI uses advanced security technologies to keep your data safe and secure and keeps upgrading them to meet emerging security threats and challenges.

MISSION KASHI

our pilot project on Universal Health coverage

Come & join the movement. Your Support is important to us.

Register, Donate & Sponsor at:

www.safemedicinesindia.in
or
www.jagograhakjago.com

Sri Anandamayi Ma
श्री श्री आनंदमयी माँ

24X7 toll free 1800-11-4424

PATIENT SAFETY AND ACCESS INITIATIVE OF INDIA FOUNDATION

a Partnership for Safe Medicines India Initiative

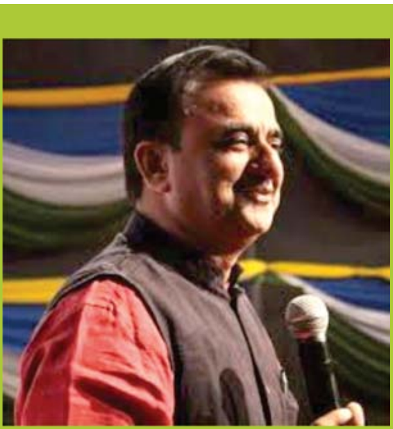
संपूर्ण स्वस्थ्य कव्रिज . गुणवतपूर्ण स्वस्थ्यसेवा

Promoting Internet Safety Amongst 'Netizens'

Rakshit Tandon, in personal capacity has sensitized more than 2.5 million students on the issue of Cyber Safety across the nation covering more than 26 states, 4 union territories. Played important role contributing to Child Online Protection in India.

Rakshit Tandon

Cyber Security Expert
Director- Council of Information Security



THE USE OF the internet has become an integral part of our daily lives. It has consolidated itself as a powerful platform that has revolutionised business, commerce and the way we keep in touch with friends.

The rapid growth of this information highway has also led to new forms of crime online - also termed as 'cybercrime'. Cybercrime has been used to describe a wide range of offences, including offences against computer data and systems (such as 'hacking'), computer - related forgery and fraud (such as 'phishing'), content offences (such as disseminating child pornography) and copyright offences (such as the dissemination of pirated content).

According to a report published by the Indian Computer Emergency Response Team (CERT), which is the national agency responding to computer security incidents, the number of incidents reported in 2004 were 23. In 2007, the figure went up to 1,237 and in 2010 there was a significant rise to 10,315 incidents.

The United Nations Office on Drugs and Crime (UNODC) undertakes efforts to contribute to a greater understanding of the threat of cybercrime and supports member states to act against it. In India, UNODC worked with the Ministry of Home Affairs, on action points to prevent cybercrime against children and increase internet safety for them. Mr. Rakshit Tandon, a cybercrime expert and advisor to the Cybercrime Complaint Cell, participated in this exercise and has shared his views in the following interview.

Mr. Rakshit Tandon, Cyber Security Evangelist has experience of more than a decade in Security Domain. Chairing and part of various Important Security Councils and Chapter. He is Director Executive - Council of Information Security and Cyber Security Consultant to Internet and Mobile Association of India. Marked as Resource Person/Faculty for Cyber Crime Investigations at BPRD Bureau of Police Research And Development for Training Law Enforcement Officers across the Country. Member Advisory to National Cyber Safety and Security Standards.

He in personal capacity has sensitized more than 2.5 million students on the issue of Cyber Safety across the nation covering more than 26 states, 4 union territories. Played important role contributing to Child Online Protection in India Report by UNICEF. Has been Non European Expert at European Commission on Safer Internet in 2010.

Some excerpts from his interview.

Q India has seen a steady increase in cybercrime, what would the reasons for that be?

According to a reportpublished by Norton, approximately 30 million people in India were victim to cybercrime and the country witnessed a record loss of 4 billion dollars. The primary reason for this is cyber illiteracy.

The Internet penetrated into our country very fast and we were not educated on how to use the internet. Our cyber education started from cyber cafes, where we only learnt how to use sites like Google, Orkut and Facebook. We were never taught important things like the protocols of the internet and digital safety.

For example, online banking sites often have a virtual keyboard which should be used to enter information, but very few people use it. The virtual keyboard protects the computer from Trojan viruses, that act like key loggers accessing information that is typed in. However, very few 'netizens' are aware of this and are therefore, making themselves vulnerable to identity theft online.

Q How vulnerable are children to cybercrime? Have social networking sites affected cybercrime amongst children?

Children are highly vulnerable to cybercrime and this is an issue of serious concern. I read a newspaper article stating that in India, 32% of the parents say that their children have had a negative experience online. These experiences include cyber bullying, 'eve teasing', impersonation and child pornography.

Children as young as 11 years are now on Facebook, even though Facebook says that the social networking site is meant for 13 year olds and above. Children don't know how to properly use social media. They may unknowingly post compromising pictures of themselves, which then are morphed and used to cyber bully them.

Q What advice would you give parents and children to help them guard against cybercrime?

Both parents and children need to be educated on how to be cyber smart. The internet is not a scary place, but it is misused. 'Netizens' need to learn 'netiquettes', the lack of which is making them vulnerable online.

For example: A 14 year old girl came to me and said that her email account had been hacked. I recovered the account for her, but again the next day she came to me with the same problem. I once again recovered the account, but was curious to know why her account was being hacked so frequently. I looked at her sent items and was shocked to see that she was sharing semi-nude pictures of herself with an 18 yearold boy. Her account was being hacked by one of her classmates to access these pictures.

These are very common occurrences amongst children and they need to be made aware of what is appropriate to share online. Schools need to conduct classes where children learn about using the internet wisely. Issues like cyber bullying and cyber stalking need to be addressed. We need helplines where children can call and immediately be advised on such matters.

Children are highly vulnerable to cybercrime and this is an issue of serious concern. In India, 32% of the parents say that their children have had a negative experience online. These experiences include cyber bullying, 'eve teasing', impersonation and child pornography.

Q How is the Government of India handling issues relating to cybercrime?

The Government has started educating the police on issues relating to cybercrime.Training modules focusing on mobile surveillance, tracing anonymous emails, phishing etc are being conducted. Cyber cells and cyber forensic labs are being established in every state. Special law enforcement training for child related cybercrime is also underway. Apart from this, the Department of Telecommunication (DOT) and Information Technology (DIT) are aggressively promoting child - parent safety through their online portals.

Law enforcement agencies together with parents and children are trying to create a secure environment online, where cybercrime is minimized.

Pyush Misra
Director,
Consumer Online Foundation

Is It Safe to Have Your Browser Remember Your Passwords?

LET'S BE HONEST - not all of us have the best memories. This makes the ability for many browsers to remember our passwords seem like a godsend. However, is this capability actually a good thing for your cybersecurity? The answer may not surprise you.

Nope!

While yes, the fact that we no longer have to remember each different password for our online accounts may seem ideal, relying on the browser to remember them for us presents a few issues. Each of these browsers leaves some kind of opening for a hacker to review a user's list of passwords.

Google Chrome - When a user is logged into their Google account, Chrome will automatically save any passwords that user inputs. If a hacker was then able to gain access to that Google account, the entire list of passwords would be available to them.

Mozilla Firefox - Utilizing low-level encryption, Firefox hides a user's passwords, utilizing a single master password as the encryption key. However, because this encryption has such a low level, a brute force attack can break it. Plus, if someone is in possession of the device itself, they can access the passwords without having to log in.

Safari - Just as is the case with Firefox, Safari stores all passwords in the browser's settings, where they can be accessed without a login required.

Internet Explorer - When Internet Explorer saves passwords, all it takes to expose them is a readily available tool.

Microsoft Edge - Edge has had some security issues, such as a flaw that enabled hackers to read files that were browser-compatible (like the notepad files that some might keep a list of passwords in). In addition, some third-party password managers, like Edge Password Manager, have failed to require password authentication in the past.

Of course, there are other threats to your password security as well. For instance, a bug that dates back 11 years was discovered early this year that allowed website credentials to be stolen. A secondary form was hidden behind the login form, stealing usernames (which were often just the user's email) and passwords without the user having any idea.

What Can Be Done?

Your first step should be to disable your preferred browser's built-in password manager.

Google Chrome - Under the toolbar, select Chrome Menu, and from there, Settings. Scroll down until you can select Advanced, and from there, select Manage passwords (found under Passwords and forms). Finally, switch Auto Sign-in to off.

Mozilla Firefox - In the toolbar's Firefox Menu, access Options. On the left, access Privacy & Security, and find Forms & Passwords. Find the Remember logins and passwords for websites option and deselect it.

Safari - Select Safari Menu from the toolbar, and then select Preferences and Autofill. Then you'll need to deselect Using info from my Address Book card, Usernames and passwords, and Other forms.

Internet Explorer - First, you need to reconsider utilizing Internet Explorer, assuming your organization gives you a choice in the matter. If you must, you will want to access the toolbar's Internet Explorer Menu and select Internet Options. From there, click into Content, and select Settings (found under AutoComplete). Deselect both Forms and Searches and User names and passwords on forms. Finally, save your changes by clicking OK.

Microsoft Edge - Again, from the toolbar, select Edge Menu and from there, Settings. Scroll down to find View advanced settings. Under Privacy and services, deactivate Offer to save passwords, and under Manage passwords, deactivate Save from entries.

We understand, remembering all of your different passwords can be a real pain, but relying on your browser to remember them just isn't a good option. There are, however, services like LastPass that can store your passwords much more safely behind much more powerful encryption. While these solutions aren't infallible either, they are a much better choice than entrusting your browser. ◗

THE AWARE CONSUMER

An opportunity to SPEAKUP!

Join the Movement ...

Save upto **50%** on subscription

Subscribe today!

{Save ₹3,600/- FOR 36 ISSUES}

India's more credible consumer monthly from renowned Consumer Activist Bejon Kumar Misra

Please accept my subscription of **THE AWARE CONSUMER**

NAME ______________________________

ADDRESS ______________________________

PH. NO. ______________ E-MAIL ______________

PAYMENT □ CASH □ CHEQUE CHEQUE/DD NO. ______________

DRAWN ON ______________________________

DATE ______________ SIGNATURE ______________

No. of Issues	News Stand Price	Discount	You Pay	You Save
12	₹ 2,400/-	20%	₹ 1,920/-	₹ 480/-
24	₹ 4,800/-	30%	₹ 3,360/-	₹ 1,440/-
36	₹ 7,200/-	50%	₹ 3,600/-	₹ 3,600/-

Cheque / DDs should be drawn in favour of **BEJON KUMAR MISRA**
Send your subscription to: The AWARE CONSUMER, F-9, 2nd Floor, Kailash Colony, New Delhi-110048
Contact: 9811044424 • +91-11-40537140 • E-mail: bejonmisra@gmail.com

5 million preventable deaths occur every year

Helpline

1800-11-0456

Reach out to us before you are one of them

SAFETY IS YOUR BUSINESS

How To Stay Safe From Online Financial Fraud

Fraudsters have devised many ways of stealing sensitive information from you, so they may eventually steal hard cash and wealth. Here are some of their tricks

– Shaikh Zoaib Saleem

DID YOU KNOW that every time you swipe a card, you may be exposing yourself to a hacker or a fraudster? Recently the Reserve Bank of India (RBI) said that there has been a surge in grievances relating to unauthorised transactions. In 2016, banks reported multiple instances of data breaches, especially with debit and ATM cards. In 2013, too, banks had reported several instances where Indian credit cards were used fraudulently from websites overseas—while, even today, many online fraudulent transactions remain unreported. However, that doesn't mean you should stop electronic transactions.

With increasing usage of devices connected to the internet, we are constantly at the risk of being trapped by fraudsters. The damage to an individual or an organisation can be reputational as well as financial. The most common type of theft online is identity theft.

While identity theft in itself can be harmless, often it is only the first step of causing larger damages such as stealing critical information or money from your bank accounts. Though it is not impossible to execute a hack and steal money from a bank account remotely, often some kind of physical involvement at some stage is needed. We spoke to experts to understand how some of these tricks work, so that you can be more careful and not fall into traps.

SIM card cloning

Most financial and non-financial transactions need a one-time password, which you receive on your registered mobile phone. This is a crucial detail. We freely give photocopies of our identity proof and PAN card wherever needed. Sometimes, these end up in wrong hands and they are able to get a SIM card for your number using these documents. If you have not given an alternate number to the telecom company, you have no way of finding out that a new SIM card has been issued. If the service provider has another number to contact you, you can be alerted that there is a request from you for a new SIM card.

When a new SIM gets activated, the one that you have gets disconnected.It should be alarming, but what happens in reality is that when network disappears from your phone, your first reaction is that there is some problem with the network. However, Aadhaar-based verification is helping solve this problem to quite an extent.

Social engineering

Social engineering in the context of frauds means manipulating a person in such a way that she gives out information that can be used to commit fraud. Usually, individual or sets of individuals are identified as targets. Through just social engineering, you can get a lot of private information on an individual. An attempt is made on thousands of people and the hit rate is 2-3 in a thousand.

It is not uncommon to find basic details like name, date of birth, address, email and phone numbers online. Data sets according to age, location, salary or other metrics are sold in the market. Along with some more technical steps and social engineering, this information can be used to hack someone. For example, if you are using an email service, there are some security questions you have to answer to recover a password. Some of these questions, like mother's maiden name or first school you attended, are used in many places. So, social engineering is used to get answers to your security questions. And the answers are then used to get into, say, your account.

Malware

These are programs that steal information while hiding somewhere on your device. People want to download a lot of free software, videos and music; and chances are high that those files are hosting some malware that will steal information from the end machine.These can also get downloaded to your device when you click on some link, usually in spam emails or SMSs promising something attractive, cheap or free.

The inherent nature of malware is to steal information from the device. The malware is coded to pick up information from the device and send it to the command and control centre, which is hosted somewhere on the internet. Malware is designed smartly and does not look for non-sensitive information. It looks for sensitive information based on keywords like password, banking, or transaction. Any file having these keywords is stolen.

An advanced version of malware is ransomware. This does not even steal information. It just encrypts the data so that you cannot access it. If you want to access it, you have to pay a ransom. To avoid ransomware risk, it is a good practice to backup of your data on an external drive, which is not connected to the internet.

How to report fraud

To ensure that banks provide more protection to customers' electronic transactions, the Reserve Bank of India issued a notification on customer protection in case of electronic banking transaction.

The RBI has clearly spelt out banks' as well as customers' liabilities in case of unauthorised electronic banking transactions. Here is what it means.

Quick response

Imagine you get a message from your bank saying Rs25,000 is debited from your account. However, you didn't do the transaction. Your immediate response may be to call your bank, send an email or maybe even visit a branch.

The RBI's notification wants banks to provide more options for reporting fraudulent transaction immediately. For instance, today when you get an SMS or an email about a transaction, you cannot reply to it. The RBI has asked banks to enable services so that customers can instantly respond by replying to the SMS or email alerts they get from banks. Soon you may be able to respond instantly to any SMS that you believe could be about a fraudulent transaction. The regulator has also asked banks to provide a direct link for lodging complaints, with a specific option to report unauthorised electronic transactions on the home page of banks' websites. Currently, you don't have this option on the home page. For the things that RBI has listed, all banks will have to work with their core banking teams that looks at protocols on intimations. They also have to give details to the vendors. Hence, it will take time for banks to make these changes.

Reporting timeline

Reporting a fraud is the first step to dealing with it. The regulator has given a structure on how to do it. Bankers say that these reporting requirements existed earlier also but now there is a standard time frame for reporting them, and your liability is linked to the timeline.

To begin with, if an unauthorised transaction takes place and the bank is responsible for it, then even if the customer doesn't report the fraud, the customer has zero liability. This means the bank will make good any losses you may incur. Most banks take an insurance on fraudulent attacks such as skimming and hence the customers' liability too gets limited when it gets reported.

Now, say there is a third-party breach where neither the bank nor the customer is responsible and the customer responds within 3 working days. Then too the customer doesn't have any liability. But in case you don't report the fraud within 3 days but within 4 to 7 working days after receiving the communication from the bank, you will have limited liability for the transaction. Limited liability means you will incur some monetary loss for the fraud.

But what if you report after 7 days? In such a situation the bank will decide what to do. While these policies will vary from bank to bank, all banks have been asked to put details of their policy in the public domain and also inform customers about it individually. Remember that the above timeline starts after the day complaint was made. And the working days are counted based on the schedule of the home branch. Also, once reported, the RBI has asked banks to resolve the case within 90 days from the date of receipt of the complaint.

The cost

In cases where you share responsibility for a fraudulent transaction, or you have limited liability due to late reporting, the central bank has listed out the liabilities in detail. If the loss is due to your negligence, you bear the entire loss till the time it was reported to the bank. For instance, if you have shared your PIN or password with anyone and the money was stolen, you have to bear the loss. But even in such cases, any loss occurring after the reporting of the unauthorised transaction will be borne by the bank. Wherever you have limited liability, the amounts have been capped in the range of Rs5,000-25,000. The amount depends on the kind of account you use. For instance, for a basic savings account, the liability is capped at Rs5,000. For other savings accounts, prepaid instruments, gift cards, and credit cards with limits of up to Rs5 lakh, your liability is limited to Rs10,000. For credit cards with limits above Rs5 lakh, liability is capped at Rs25,000.

Now, what happens to the money that gets lost due to the fraudulent transactions? Once you inform the bank, the bank has to credit the amount involved in the unauthorised electronic transaction to your account within 10 working days from the date you raise the alert. In case of debit card or bank account fraud, the customer does not suffer loss of interest. In case of credit cards, the customer does not bear any additional burden of interest.

What you should do

Just because roads are prone to accidents, do you stop driving on the road? To avoid accidents, you take safety measures and follow the rules. Similarly, you should protect yourself from frauds in case of online transactions.

How can you do this? If you use online transactions or swipe cards, you should sign up for all the SMS and email alerts for electronic banking transactions. This is the easiest way to know if there has been any movement in your account. In case of any unauthorised transaction, you should immediately inform your bank. When you register a complaint, banks record its time and date, which is important to determine the extent of your liability. Hence, ensure that you don't delay the process.

Being alert, and even before that, following basic rules like not storing passwords and PINs, having complex and different passwords for different services, not clicking on unknown links and not downloading from suspicious sources can keep you safe to a large extent. ◗

Banking "SMART"

Smartphone users today have round-the-clock access to their bank accounts and literally carry their bank in their pockets.

– Sanjeev Sinha

WITH EACH PASSING day, banking is becoming simpler. From those old long queues in front of the teller's counter to today's mobile applications, where most banking transactions are possible with the click of a button, banking has come a long way -- thanks to technology and the advent of that clever small device called 'smartphone'.

Smartphone users today have round-the-clock access to their bank accounts and literally carry their bank in their pockets. But banking with your smartphone also requires applying common sense and staying informed about the threats to your mobile security.

Security Tips to bank with your smartphone

Mobile banking makes your life easier, but it can also pose a threat to your mobile security, if you don't use it carefully. Therefore, before you start using your smartphone as the preferred banking tool, here are some security tips to keep in mind:

■ **Download Banking Applications:** Gone are the days when smartphone users had to do mobile banking through browsers on their phones. Today, all banks offer customized banking applications, or 'apps', for various handheld devices. Different versions of apps are available for Android, iOS and Blackberry smartphones, and depending on the phone's operating system, one can install the recommended version.

"Banking apps not only offer a faster interface, but also have a higher security layer, including password protection. If you need to transfer funds to any other bank accounts, funds transfer is only a click away using mobile banking apps, giving you full flexibility to move your funds even as you are on the move," says Adhil Shetty, CEO, BankBazaar.com.

■ **Use Mobile Wallets:** Many users are purchasing goods and services over the internet, but are paying for them through credit cards or bank transfers. Fund transfers through Mobile Wallets are the latest novelty in this class of transactions. Mobile Wallets are pre-paid virtual cards. You can load it with money and use it for bill payments, e-shopping, fund transfer etc. Some m-wallets not only make payments easier, but also offer lucrative discounted deals for future purchase.

Following in the footsteps of telecom giants Airtel and Vodafone, who offer 'Airtel Money' and 'Vodaphone Pesa', a handful of mobile wallet players like PayTM, MobiKwik and Oxigen are quickly gaining popularity among e-shoppers. PayTM, for instance, offers transfer of funds from wallets to bank accounts. ICICI Bank has launched their wallet 'Pockets', even as HDFC has come up with 'Chillr'. While users of Pockets need not be ICICI account holders, Chillr is open for HDFC account holders only.

■ **Use Call-to-Pay / IVR Services of Banks:** If you are caught in a situation where the net connection on your phone is down, or if you are unable to access the banking app on your smartphone, IVR and Call-to-Pay are the other options. These services can be used to check account balance, do fund transfers and conduct other transactions.

"The banks offering these services are using voice recognition software, ensuring safe and secure transactions for account holders. However, there are some limitations for these services as they are restricted to the above mentioned only," observes Shetty.

■ **Payment Bank Concept:** The Government of India is aspiring to make basic banking transactions available for everyone in India through the Payment Bank concept. This concept of 'anywhere, anytime banking' is also aimed at tapping mobile phone users, to offer banking transactions over phone for the common person. This is planned to operate through mobile wallets providers, telecom providers, retailers and others to reach out to the millions of mobile users who are unbanked.

■ **Banking Through Social Media:** Apart from the above, banking through social media, which can be carried out on your mobile phone, is also creating a buzz. In India, ICICI Bank is offering fund transfer via Twitter, while Kotak Bank's app Kaypay facilitates fund transfer via Facebook. Third party wallet providers like Oxigen are providing fund transfer facility via Facebook, Twitter, and WhatsApp, while HotRemit is offering services for BBM users.

Apart from these, you can also do some other things related to banking, like locating bank ATMs. "When you are traveling or looking for an ATM that won't charge you a surcharge, mobile banking offers you the best way to get to the nearest ATM. Using your phone's GPS, a bank app can provide you the nearest network ATMs and save you money," says Siddharth Arora, CEO & Co-Founder, ePaisa.

■ **Keep the Banking App Updated:** Updating the banking app whenever a new version is available is a must-do. App developers keep adding various new security features and bug fixes, which are released as updates periodically.

"The best way to ensure periodical updates is to give the application permission to install the latest updates automatically as and when they are released. You can also switch on the 'push notifications' feature to know whenever an updated version is available," informs Shetty.

■ **Avoid Using Public Wi-Fi Networks:** While banking apps have strong security mechanisms, it is prudent to avoid using public Wi-Fi networks for banking transactions.

Citing the reason, Shetty says that public Wi-Fi networks can be infected with Trojans and hidden viruses that can potentially steal information from smartphones. So, "always make sure that you are connected to a secure Wi-Fi network," he says.

■ **Avoid Automatic Logins:** Don't allow your browser or app to save your banking passwords -- on the web or on a mobile app. "Automatic logins are convenient, but very dangerous if they come in the wrong hands. Otherwise, if a phone is lost or stolen, someone may have access to all your data, and your money," informs Arora.

■ **Don't Save Your Login Credentials:** Don't share your passwords, pins, answers to secret questions or store them anywhere on your handset. Saving your login credentials in your address book is a bad idea.

■ **Keep Track of Your Device:** Take special care to make your phone traceable. Smartphone manufacturers offer various features to track the phone or render it unusable in situations like theft or misplacement. These include features like auto-locking, finger-print recognition, etc.

■ **Clear Data Periodically:** Banks send information for every financial transaction, including text messages with one-time passwords to validate any transaction. "Make sure you clear all such data periodically to avoid leakage of any sensitive information to any third party at any point," says Shetty.

As mobile banking gains in popularity, it is expected to push the boundaries of possible transactions to a wide range of related services like loan approvals, mutual fund purchases, and many more in the days to come. While this bodes well for the smartphone user, it brings with it an additional responsibility – that of keeping your phone safe from hackers and intrusive technology! ◗

SLAMMING THE WEB WORM

Internet Viruses

Spurred by the prevalence of always-on, high-speed connections, the Internet has become a powerful tool for enhancing innovation and productivity. The increasing dependence on the Internet and other communication networks, however, means the Internet has also become a popular and efficient way to spread computer viruses and other types of malicious software (malware).

"Viruses", "worms" and "zombies" might sound like science fiction, but they are in fact the reality presented by the spread of malware. The power and threat of malware are that it can infiltrate, manipulate or damage individual computers, as well as entire electronic information networks, without users knowing anything is amiss. All of this has brought the electronic world to an important juncture.

MALWARE ATTACKS ARE increasing in both frequency and sophistication, thus posing a serious threat to the Internet economy and to national security. Concurrently, efforts to fight malware are not up to the task of addressing this growing global threat; malware response and mitigation efforts are essentially fragmented, local and mainly reactive.

A wide range of communities and actors – from policy makers to Internet Service Providers to end users – all play a role in combating malware. But there is still limited knowledge, understanding, organisation and delineation of the roles and responsibilities of each of these actors. Improvements can be made in many areas, and international co-operation would benefit greatly in areas such as: proactive prevention (education, guidelines and standards, research and development); improved legal frameworks; stronger law enforcement; improved tech industry practices; and better alignment of economic incentives with societal benefits.

Without a reliable antivirus program on your PC and devices, you're at the mercy of a huge range of programs that can adversely affect your computer. It's not always easy to tell if your computer has been infected with a virus, spyware, malware or other cyberspace vermin, but here are a few telltale clues: your PC runs slower than normal, freezes without warning, has strange pop-up windows appear out of nowhere or just doesn't behave normally all of a sudden.

Invest in a top-notch antivirus system to reduce future problems. This is particularly important for computers used in the running of your business.

With thousands of new online viruses appearing daily, it's impossible to protect yourself against everything, but a decent antivirus program (designed to handle a wide range of threats) is a good start. Quality antivirus software can be regularly updated so you can protect yourself against new 'strains'.

Beware of free antivirus systems that you're invited to download over the Internet – these are often the quickest way to find yourself infected with a new virus! Go to a software store and buy packaged software instead. An internet security suite that offers a firewall as well as antivirus and ant-spyware protection is ideal.

Regularly delete your temporary Internet files. Aside from freeing up space on your hard drive, this also speeds up virus scanning and may even remove basic spyware.

If you believe your system has been infected, you'll find numerous tips online on the most effective ways to remove them. Once you've rid yourself of the offending virus, make sure you change all your passwords and usernames. Invest in a top-notch antivirus system to reduce future problems. This is particularly important for computers used in the running of your business.

Be aware that being connected to the Internet is not needed to become infected with a virus – some viruses can be transferred through documents or other files hidden on a CD you've borrowed from a friend. ◗

THE MOST FAMOUS INTERNET VIRUSES

SOME VIRUSES WERE created by accident, others with the intention of committing cybercrimes. History records the top 10 minds who created viruses and caused damage to both people and businesses. In addition, of course, some damage to the privacy of victims who have had their personal data hacked and disseminated on the Internet.

And who is behind the creation of these viruses ? Learn the history of the 10 most destructive viruses of today and its creators:

ELK CLONER

A first of its kind, in 1982, the Elk Cloner didn't harm a lot of computers, but it did set an unsettling precedent as the first wild virus, one that can freely spread on its own. Created by Richard Skrenta, a computer savvy high school prankster, it merely infected boot sectors, featuring a threatening message that read “It will get on all your disks. It will infiltrate your chips. Yes it's Cloner!” Fittingly, Skrenta is now a computer programmer and Silicon Valley entrepreneur with extensive experience in the industry.

Brain

Viruses were made more complicated and resilient with the formation of Brain, in 1986, the first full-stealth virus capable of evading early disk utility programs. Infecting floppy disks, it caused only minor problems, as it slowed the disks and sometimes made them unusable. Brain originated in Lahore, Pakistan and its effects surfaced in 1987 and 1988, when infections were discovered at the University of Delaware and the Providence Journal-Bulletin, the latter of which experienced the deletion of work as a result. Today's viruses that refuse to die are all grandchildren of Brain, which is why it will forever be considered among the most disruptive — it bred them.

Morris Worm

The story goes that the virus was created by Robert Morris in 1988. It was developed without the intent to commit cybercrimes. In fact, Morris tried to measure the size of the Internet. From a flaw in software code, millions of computers to NASA were infected, paralyzing all network resources around the world.

CIH

This virus was created in 1998 by Chen Ing Hau. He was also known as Chernobyl.Considered the most devastating compared to other viruses, CIH was able to delete data from the infected computer and, in some cases causing a total machine loss.

Melissa

In 1999, David L. Smith created the Melissa. The virus was sent by email and had the ability to multiply in Word, Excel and Outlook. Where Melissa went on , It turned off all e-mail systems, causing an overload on the internet servers.

I Love You

Unromantic, a developer of Manila, the Philippine capital, created the virus 'I love you' in 2000. This was a more problematic spread around the world.

Users received an email named 'I love you'. In addition to ordinary people, many government agencies have been attacked, including the CIA. It had to stop using your email system to stop proliferation.

Code Red

This virus was created in 2001, probably in China. Won the name eEye Digital when the researchers discovered. At the time, they were tdrinking something called Code Red Mountain Dew. Code Red infected systems that were running the server software and left the following message: “Hacked by Chinese!”

Nimda

Created in 2001 by an unknown, Nimda used different means to propagate. The result was a very slow Internet connection. Nimda was considered the fastest worm in history, taking only 22 minutes to be on the Internet and spread rapidly around the world. Nimda's name comes from the word “admin”, making mention of server administrators who challenged the virus.

Slammer

This virus in 2003 left South Korea without Internet for 12 hours. The

```
public static class ModelVisual3D...
{
    public static void AddGeometry(this ModelVisual3D visual, GeometryModel3D geometry)
    {
        if (visual.Content == null)
            visual.Content = geometry;
        else
        {
        //Check if Model3D are a group
            if (visual.Content is Model3DGroup)
            {
            //Get the first geometry
                var m3D = (GeometryModel3D)((Model3DGroup)visual.Content).Children.First();
                MeshGeometry3D main = (MeshGeometry3D)(m3D.Geometry);
                MeshGeometry3D toAdd = (MeshGeometry3D)(geometry.Geometry);
                Point3DCollection pc = new Point3DCollection(main.Positions.Count + toAdd.Positions.Count);

            //Get all Point3D from mesh
            foreach (var pt in main.Positions) pc.Add(pt);

            //Apply transform data before adding to collection
                foreach (var pt in toAdd.Positions)
                {
                    pc.Add(geometry.Transform.Transform(pt));
                }
                main.Positions = pc;

                Vector3DCollection vc = new Vector3DCollection(main.Normals.Count + toAdd.Normals.Count);
                foreach (var v in main.Normals) vc.Add(v);
                foreach (var norm in toAdd.Normals) vc.Add(norm);
                main.Normals = vc;
```

Slammer took advantage of the weakness in Microsoft SQL Server to infect, making computers inoperable.

Blaster

It was created by the Chinese hacker group called Xfocus in 2003 in order to attack Microsoft Windows systems. Wherever it went, left the following message: "Bill Gates why do you make this possible. Stop making money and fix your software !!?"

Sasser

Sven Jaschan created the virus in 2004. He attacked computers running Windows operating system. He became famous also for having been responsible for the cancellation of the flight of Delta Airlines, stopped Coast Guard map services of England and cut communication satellite for the France-Press news agency.

MyDoom

According to some sources, MyDoom in 2004 is the most destructive and costly worm in the history of the Internet, causing $38.5 billion in damage and effecting 20 to 30 percent of worldwide email traffic. Rapidly spread through email and the popular file sharing application Kazaa, it presented itself as a transmission error and spread to other emails by prompting readers to open its attachment. As with the Blaster Worm episode, the creator of MyDoom wasn't found, but some have speculated that he or she was paid and lived in Russia.

Storm Worm

In 2007 this virus was identified as a fast spreading email spamming threat to Microsoft systems. It begins gathering infected computers into the Storm botnet. By around June 30 it had infected 1.7 million computers, and it had compromised between 1 and 10 million computers by September.[40] Thought to have originated from Russia, it disguises itself as a news email containing a film about bogus news stories asking you to download the attachment which it claims is a film.

Here You Have

The virus, called "here you have" or "VBMania", is a simple Trojan horse that arrived in the inbox in 2010 with the odd-but-suggestive subject line "here you have". The body reads "This is The Document I told you about, you can find it Here" or "This is The Free Download Sex Movies, you can find it Here".

Flame

Flame, also known as Flamer, SkyWIper and Skywiper, is a virus created in 2012. The creator is unknown. It attacks computers operating with Windows and has been used for cyber espionage in the Middle East.

The virus is able to record audio, take screenshots, activate keyboard and network traffic, and you can control data transfer devices such as Bluetooth. All information collected on the computers invaded are sent to multiple servers around the world.

MEMZ

The creator, Leurak, explained that the trojan in 2016 was intended as a funny joke,and warns the user that if they proceed, the computer may no longer be usable. It contains complex payloads that corrupt the system, displaying artifacts on the screen as it runs. Once run, the application cannot be closed without causing further damage to the computer, which will stop functioning properly regardless. When the computer is restarted, in place of the bootsplash is a message that reads "Your computer has been trashed by the MEMZ Trojan. Now enjoy the Nyan cat…", which follows with an animation of the Nyan Cat.

WannaCry ransomware attack

Exploits revealed in the NSA hacking toolkit leak of late 2016 were used to enable the propagation of the malware in 2017. Shortly after the news of the infections broke online, a UK cybersecurity researcher in collaboration with others found and activated a "kill switch" hidden within the ransomware, effectively halting the initial wave of its global propagation.The next day, researchers announced that they had found new variants of the malware without the kill switch. ◗

Keeping Kids Safe Online
NEED TO CARE ABOUT YOU and YOURS

CHILDREN ARE NATURALLY trusting, and this trait can make them vulnerable online. Keeping your kids cyber-safe requires education, open communication and regular monitoring. Teach them about what you do to ensure your own safety on the Internet. Make them aware of the dangers of chatting online to strangers, the need to verify the origins of emails, and what to do if they think they've accidentally downloaded a virus.

Keeping children safe online doesn't always have to be about control and restrictions.

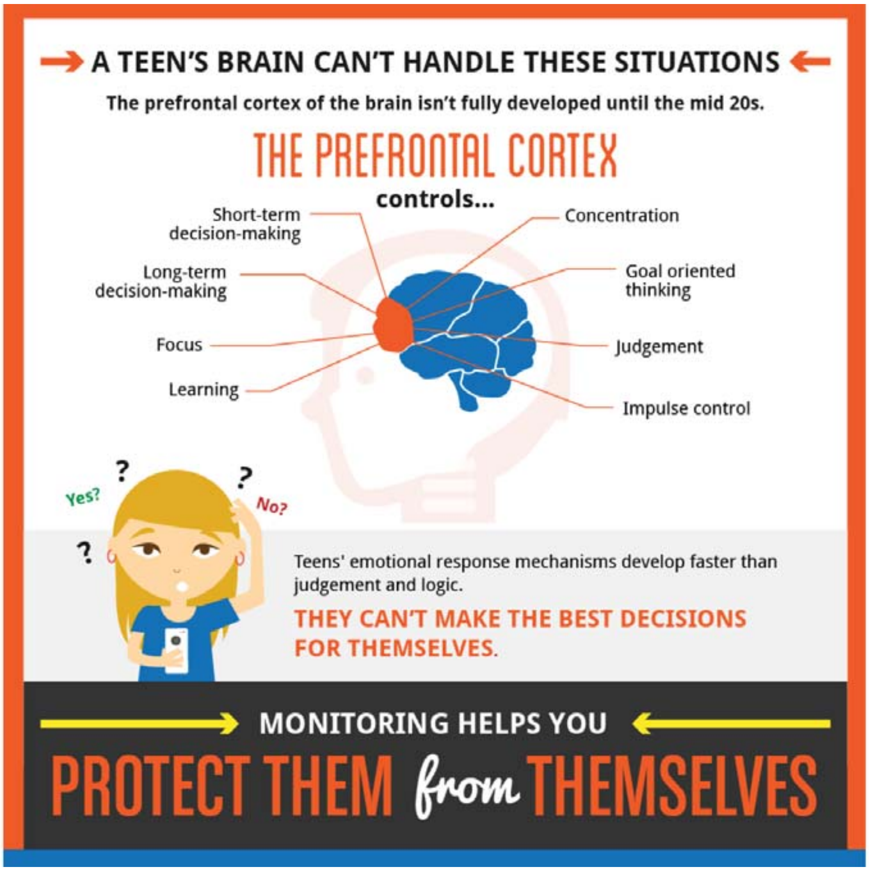
There are a number of software programs available that filter, block or otherwise control which sites your children can access. If you prefer to prevent all unsupervised browsing, you can install programs that automatically 'forget' access passwords until Mum or Dad are around to allow online access. Apps can be fun for kids, but make sure you know which ones they're using and that they're aware of the spyware dangers of downloading apps from dubious sources.

Cyberbullying is an increasing problem for children of all ages, and can be hurtful to a child's self-esteem. Teach your children never to post anything they wouldn't post if their parents were standing right behind them, and educate them about the principles of online kindness, etiquette and courtesy so they can carry good habits into adulthood.

If your child becomes a cyberbullying victim, there are a number of online resources available to help both you and your child learn about how to deal with this issue.

Like adults, children should avoid clicking on unknown email attachments and sharing their passwords. Long, run-together sentences are the easiest passwords for children to remember, and are more secure than shorter ones (like birthdays or pet nicknames).

One should always log out after they're finished with a computer (at home, at school or anywhere else) so no one can access their personal information or browsing history.



A TEEN'S BRAIN CAN'T HANDLE THESE SITUATIONS

The prefrontal cortex of the brain isn't fully developed until the mid 20s.

THE PREFRONTAL CORTEX controls...

Teens' emotional response mechanisms develop faster than judgement and logic.

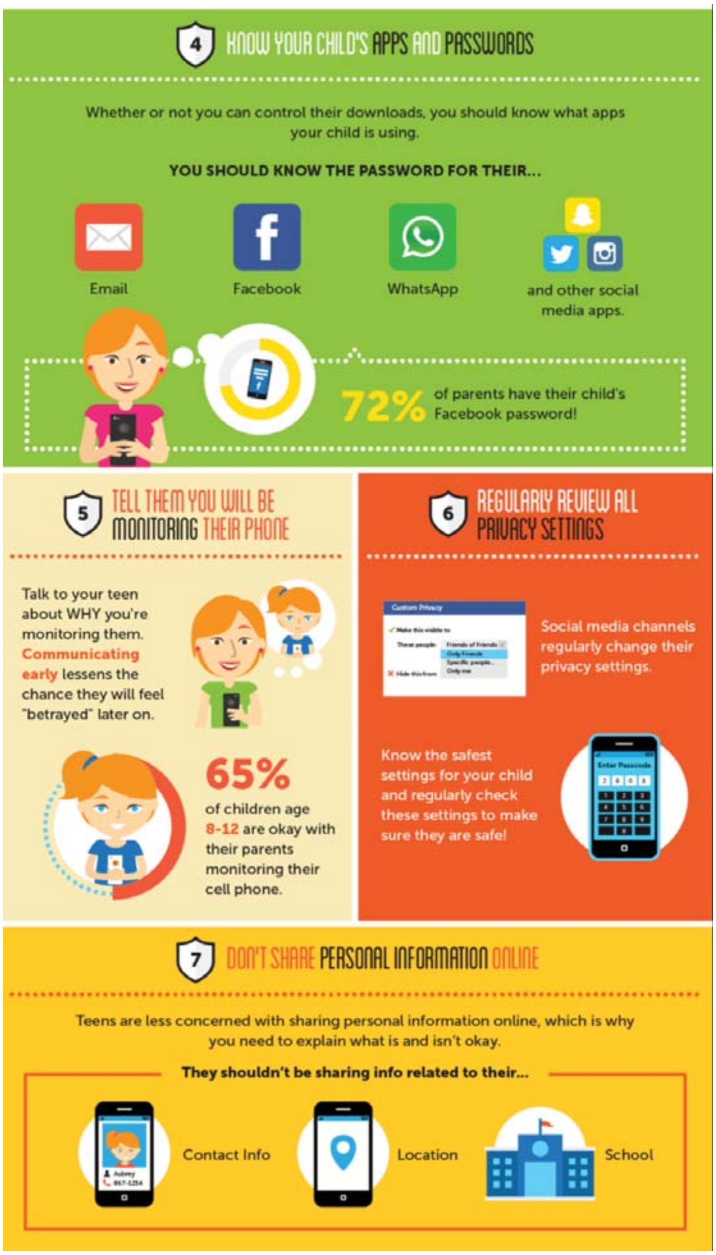
THEY CAN'T MAKE THE BEST DECISIONS FOR THEMSELVES.

MONITORING HELPS YOU

PROTECT THEM *from* THEMSELVES

6 Internet Safety Tips Every Kid Should Know

1. **Keep Your Passwords Secret**
   Except from Parents
2. **Don't Talk to Strangers**
   Only talk to people you have met in person
3. **Don't Give out Your Phone #**
   Unless parents say its okay
4. **Close and Tell an Adult**
   When you see something bad online
5. **Ask Before you Download**
   Or your computer could get sick
6. **Only Say/Share Nice Things**
   Always do kind.



4 KNOW YOUR CHILD'S APPS AND PASSWORDS

Whether or not you can control their downloads, you should know what apps your child is using.

YOU SHOULD KNOW THE PASSWORD FOR THEIR...

72% of parents have their child's Facebook password!

5 TELL THEM YOU WILL BE MONITORING THEIR PHONE

Talk to your teen about WHY you're monitoring them. Communicating early lessens the chance they will feel "betrayed" later on.

65% of children age 8-12 are okay with their parents monitoring their cell phone.

6 REGULARLY REVIEW ALL PRIVACY SETTINGS

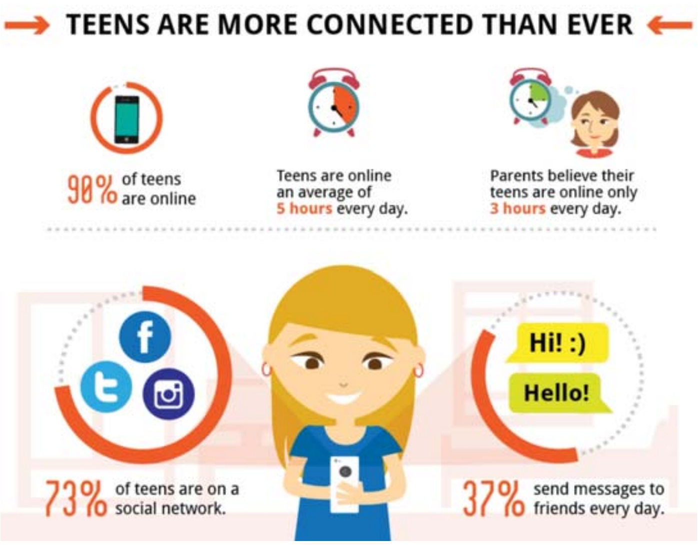
Social media channels regularly change their privacy settings.

Know the safest settings for your child and regularly check these settings to make sure they are safe!

7 DON'T SHARE PERSONAL INFORMATION ONLINE

Teens are less concerned with sharing personal information online, which is why you need to explain what is and isn't okay.

They shouldn't be sharing info related to their...



TEENS ARE MORE CONNECTED THAN EVER

90% of teens are online

Teens are online an average of 5 hours every day.

Parents believe their teens are online only 3 hours every day.

73% of teens are on a social network.

37% send messages to friends every day.

Predatory individuals will often pretend to be someone of a different age or gender in order to infiltrate a child's world. Children must be taught to connect only with people they know, and to advise their parents immediately if they're at all uncomfortable with the way an online conversation is going. Instruct them about what is and isn't acceptable when sharing photos online.

Explain to your kids that social media is not a popularity contest: it's the quality of their online friends that matters, not the quantity. And though your children (especially older ones) may not like it, you have both the right and a parental obligation to monitor their posts and online activity for their own safety. If necessary, this parental access can be a prerequisite for allowing them to go online. As they get older, you can loosen the reins as appropriate.

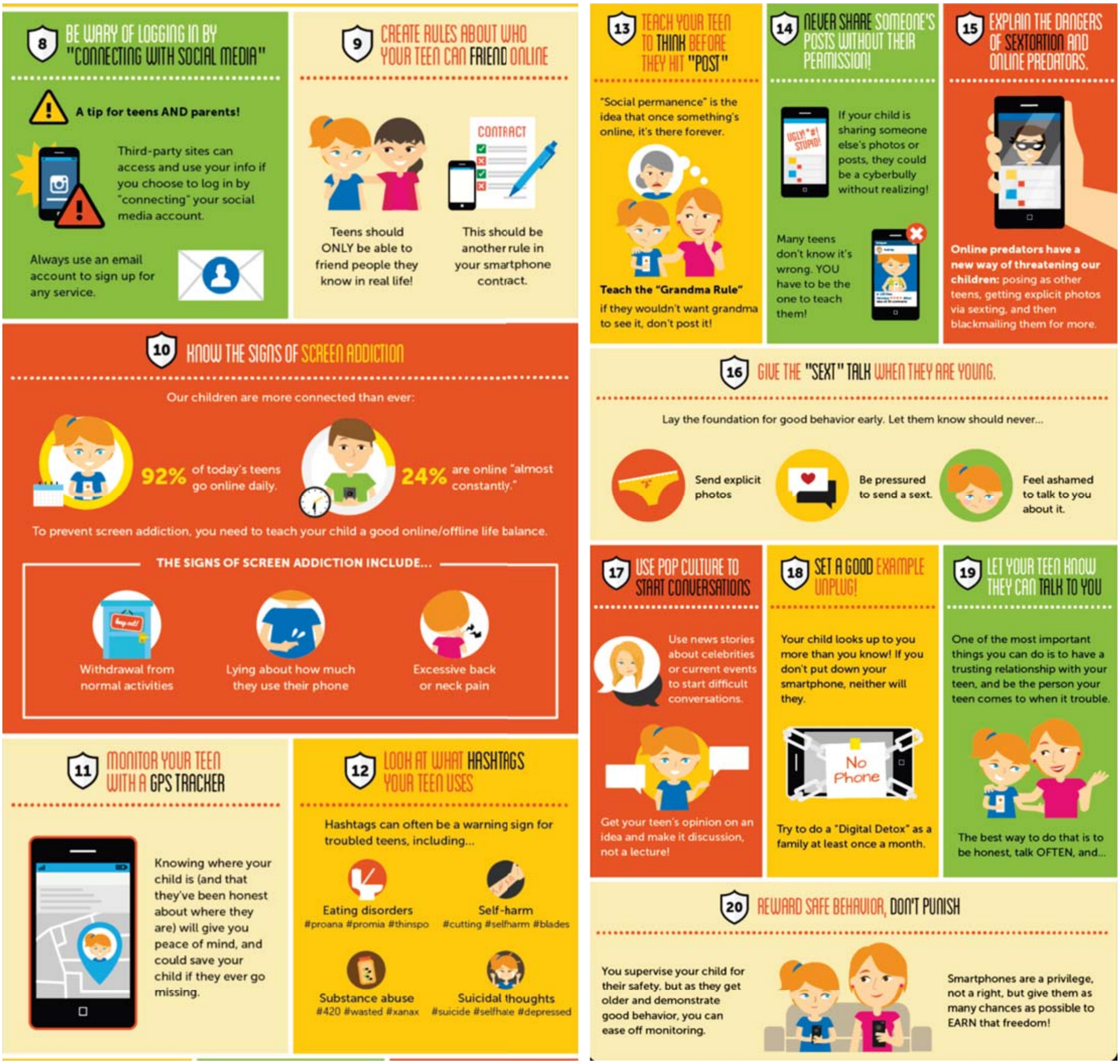
Keeping children safe online doesn't always have to be about control and restrictions. Reward them with extra online hours for doing positive things, too – like running their own security scans or changing passwords regularly.

Did you know that 65% of children age 8-12 are aware and okay with their parents monitoring their smartphone? It's all about communicating early!

How Safe Is The Mobile In The Hands Of Kids?

Giving a child a mobile phone can be a strong safety measure. After all, you can contact them whenever necessary (providing the phone is on and they answer it) and they can contact you. On the downside it also opens up a world of concerns.

While children are learning to use these Smartphones from as young as toddlers, a good time to surprise your young one with their first mobile phone is when they might be travelling alone to and from school, partaking in after school sports or may need to contact you at the last minute when plans change. Once they do receive their first device there are a few measures you can put in place for some peace of mind.



8 BE WARY OF LOGGING IN BY "CONNECTING WITH SOCIAL MEDIA"

A tip for teens AND parents!

Third-party sites can access and use your info if you choose to log in by "connecting" your social media account.

Always use an email account to sign up for any service.

9 CREATE RULES ABOUT WHO YOUR TEEN CAN FRIEND ONLINE

Teens should ONLY be able to friend people they know in real life!

This should be another rule in your smartphone contract.

10 KNOW THE SIGNS OF SCREEN ADDICTION

Our children are more connected than ever:

92% of today's teens go online daily.

24% are online "almost constantly."

To prevent screen addiction, you need to teach your child a good online/offline life balance.

THE SIGNS OF SCREEN ADDICTION INCLUDE...

Withdrawal from normal activities

Lying about how much they use their phone

Excessive back or neck pain

11 MONITOR YOUR TEEN WITH A GPS TRACKER

Knowing where your child is (and that they've been honest about where they are) will give you peace of mind, and could save your child if they ever go missing.

12 LOOK AT WHAT HASHTAGS YOUR TEEN USES

Hashtags can often be a warning sign for troubled teens, including...

Eating disorders
#proana #promia #thinspo

Self-harm
#cutting #selfharm #blades

Substance abuse
#420 #wasted #xanax

Suicidal thoughts
#suicide #selfhate #depressed

13 TEACH YOUR TEEN TO THINK BEFORE THEY HIT "POST"

"Social permanence" is the idea that once something's online, it's there forever.

Teach the "Grandma Rule"
if they wouldn't want grandma to see it, don't post it!

14 NEVER SHARE SOMEONE'S POSTS WITHOUT THEIR PERMISSION!

If your child is sharing someone else's photos or posts, they could be a cyberbully without realizing!

Many teens don't know it's wrong. YOU have to be the one to teach them!

15 EXPLAIN THE DANGERS OF SEXTORTION AND ONLINE PREDATORS.

Online predators have a new way of threatening our children: posing as other teens, getting explicit photos via sexting, and then blackmailing them for more.

16 GIVE THE "SEXT" TALK WHEN THEY ARE YOUNG.

Lay the foundation for good behavior early. Let them know should never...

Send explicit photos

Be pressured to send a sext.

Feel ashamed to talk to you about it.

17 USE POP CULTURE TO START CONVERSATIONS

Use news stories about celebrities or current events to start difficult conversations.

Get your teen's opinion on an idea and make it discussion, not a lecture!

18 SET A GOOD EXAMPLE UNPLUG!

Your child looks up to you more than you know! If you don't put down your smartphone, neither will they.

Try to do a "Digital Detox" as a family at least once a month.

19 LET YOUR TEEN KNOW THEY CAN TALK TO YOU

One of the most important things you can do is to have a trusting relationship with your teen, and be the person your teen comes to when it trouble.

The best way to do that is to be honest, talk OFTEN, and...

20 REWARD SAFE BEHAVIOR, DON'T PUNISH

You supervise your child for their safety, but as they get older and demonstrate good behavior, you can ease off monitoring.

Smartphones are a privilege, not a right, but give them as many chances as possible to EARN that freedom!

Bluetooth?

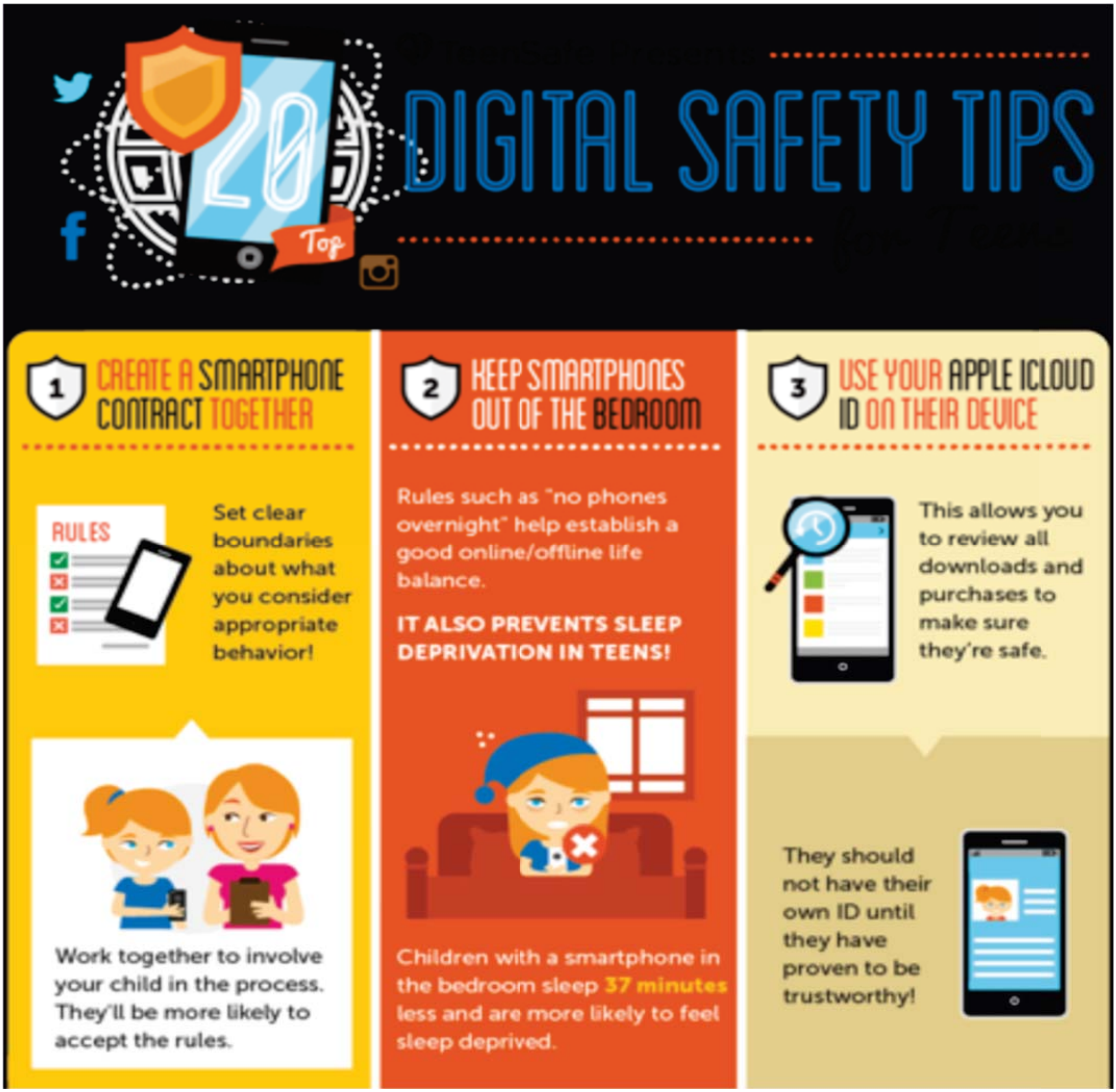
Most phones will have their Bluetooth already enabled meaning a child's mobile phone is connected to any other Bluetooth-enable phone in the vicinity. If active, your child could be open to receiving unwanted content from surrounding devices or have the privacy of their own personal content compromised. Simply switch it off in the settings menu and the problem is solved.

Registered for an adult?

If a phone is registered to a child user it will be preset to not allow access to anything rated for 18+. If this hasn't been preset it is worth contacting your mobile phone operator to put this in place or your child could find themselves stumbling across websites with adult content.

Location Services switched off?

Location Services apps effectively allow anyone using social networking devices like Facebook to know exactly where you are at any given point. This is particularly dangerous when taking a photograph and posting immediately as the phone will also attach the exact location to the photo online. This leaves a child open to stalkers who may suddenly have access to the child's



TeenSafe Presents

Top 20 DIGITAL SAFETY TIPS for Teens

1 CREATE A SMARTPHONE CONTRACT TOGETHER

Set clear boundaries about what you consider appropriate behavior!

Work together to involve your child in the process. They'll be more likely to accept the rules.

2 KEEP SMARTPHONES OUT OF THE BEDROOM

Rules such as "no phones overnight" help establish a good online/offline life balance.

IT ALSO PREVENTS SLEEP DEPRIVATION IN TEENS!

Children with a smartphone in the bedroom sleep 37 minutes less and are more likely to feel sleep deprived.

3 USE YOUR APPLE ICLOUD ID ON THEIR DEVICE

This allows you to review all downloads and purchases to make sure they're safe.

They should not have their own ID until they have proven to be trustworthy!

home address and regular haunts. This can also be changed in the general settings of the phone.

Set passwords?

Children and teens end up with a lot of personal stuff stored on their phones. Just as you wouldn't leave your laptop without a lock on it, you shouldn't leave your child's phone unprotected.

Checked school policy?

It always pays to check your child's school for information on their mobile phone policy. Are they allowed in class? Are photos able to be taken? Then ask yourself if this could put your child in danger should any photos be posted online.

Checked your bill?

Downloading ringtones, games videos and special features are all charged to your account. This can be an easy way to monitor what they might be viewing on their phones. It also wouldn't hurt to teach them to limit this behavior or you might end up with some unexpected bills at the end of the month.

A Smartphone can be the best thing you've ever given your child, but a little caution always goes a long way. ◗

सत्यमेव जयते

Department of Pharmaceuticals
Ministry of Chemicals & Fertilizers
Government of India

> The poor must have access to affordable medicines, the poor must not lose their lives because of lack of medicines... that's why Jan Aushadhi Kendras have been planned across the country
>
> नरेन्द्र मोदी

उत्तम दवाई कम दाम
स्वस्थ भारत की पहचान

WHO GMP
QUALITY ASSURED
CPSU
NABL TESTED

प्रधानमंत्री
भारतीय
जन औषधि
परियोजना

- More than **3500** functional Jan Aushadhi Kendra in 33 States/UTs
- Quality of medicines ensured by testing from NABL accredited laboratories
- Over **700** High Quality Medicines procured from WHO-GMP certified Companies
- **154** Surgical and Consumables Products
- Prices **50%-90%** less than that of branded prices

For Opening New PMBJP Kendra, please submit your application to

BPPI
Bureau of Pharma PSUs of India

Bureau of Pharma PSUs of India (BPPI)
Videocon Tower, 8th Floor,
E-1, Jhandewalan Extension,
New Delhi-110055

To locate your nearest PMBJP Kendra, Please dial Toll Free No. 1800 843 6666

Follow us on : YouTube PMBJP | @pmbjpbppi | janaushadhi.gov.in | Helpline No. 1800 180 8080

ONCE IT'S SAID, THE WEB IS FED

Safety On Social Media

PRIVACY FIRST

The importance of holding back personal information.

SOCIAL "PERMANENCE"

Once it's on the web, it's there forever.

NO REGRETS

Never send a text or photo you'll regret sending later.

GOSSIP GETS AROUND

You can end up a bully even if you don't mean to be.

- Privacy and security settings exist for a reason.
- Once posted, always posted.
- Your online reputation can be a good thing.
- Keep personal info personal.
- Know and manage your friends.
- Be honest if you're uncomfortable.
- Know what action to take.
- Keep security software current.
- Own your online presence.
- Make your password a sentence.
- Unique account, unique password.
- When in doubt, throw it out.
- Post only about others as you have them post about you.

WE USE SOCIAL media sites to keep in touch with friends, search for employment, support our favourite organisations and promote our businesses – and we do it on PCs, tablets, smartphones and a growing range of other devices.

The idea behind Internet security is to keep your personal information to yourself, while the idea behind social media is to share. This isn't a problem, provided you're careful about what you share. If you're too generous with personal details, you can become a victim of identity theft, financial fraud or burglary. Providing too much personal information can even expose you to physical danger.

Protecting your PIN numbers, passwords, credit card details and banking information is priority number one. And even though it's common to share seemingly harmless information like your birthplace or birth date on social media, this information can be used in identity theft.

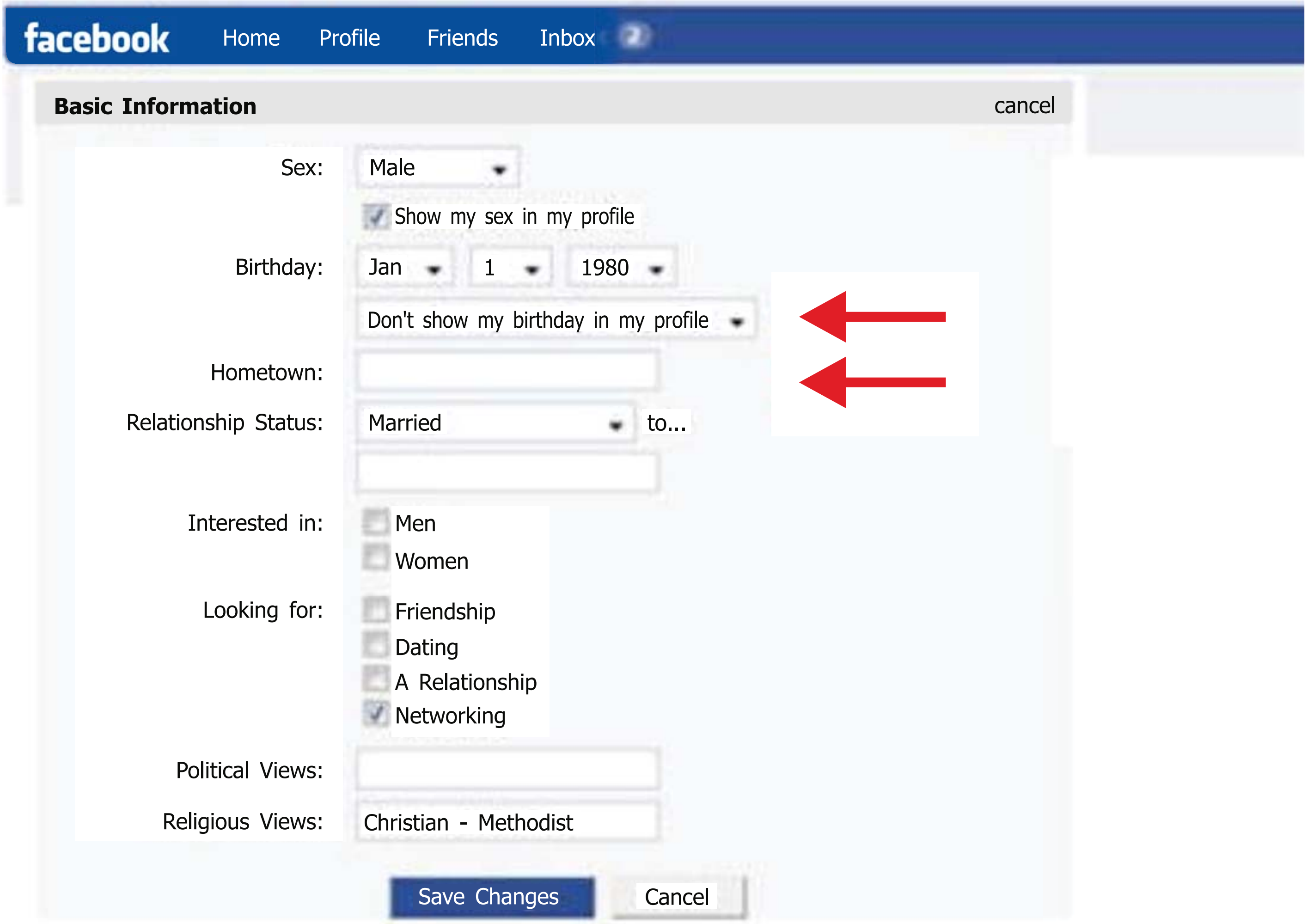
Most social media sites give you a wide range of privacy settings, so take advantage of these to protect yourself. Make sensible decisions about the individuals and groups that are allowed to view your posts.

On Linkedin, you can limit access to your contacts in relation to others in your network – a common practice for businesses that don't want competitors to steal their customer base.

Googling your own name is an easy way to check how much information is available about you online. Do this once a month or so – this also lets you know if someone is using your name for dubious purposes. It's not unheard of for people to impersonate others when replying to blog posts or conducting other online interactions, so always keep track of what's happening online in your name.

Protecting your PIN numbers, passwords, credit card details and banking information is priority number one.

It's human nature to want to tell people about your upcoming overseas holiday, or even post photos from



Basic Information cancel

Sex:	Male ☑ Show my sex in my profile
Birthday:	Jan 1 1980 Don't show my birthday in my profile
Hometown:	
Relationship Status:	Married to...
Interested in:	□ Men □ Women
Looking for:	□ Friendship □ Dating □ A Relationship ☑ Networking
Political Views:	
Religious Views:	Christian - Methodist

Save Changes Cancel

your Italian villa or the top of Machu Picchu. Resist the temptation, because burglars love it when you announce that your house is empty. Similarly, you should never let it be known that you live alone – this can give home invaders and predators all the encouragement they need. A thief that knows you're a sole occupant need merely wait for you to go head off to work before ransacking your empty abode.

And it's not just extended holidays that put you at risk: a tweet like "Taking the whole family to a resort Saturday night – can't wait!" is just as useful to burglars.

Social media is best used sparingly and with discretion.

Beware: that drunken tweet or risqué photo you were so proud of 8 years ago may still be in cyberspace when a prospective employer is looking at your online history – and deciding if you're the right person to hire.

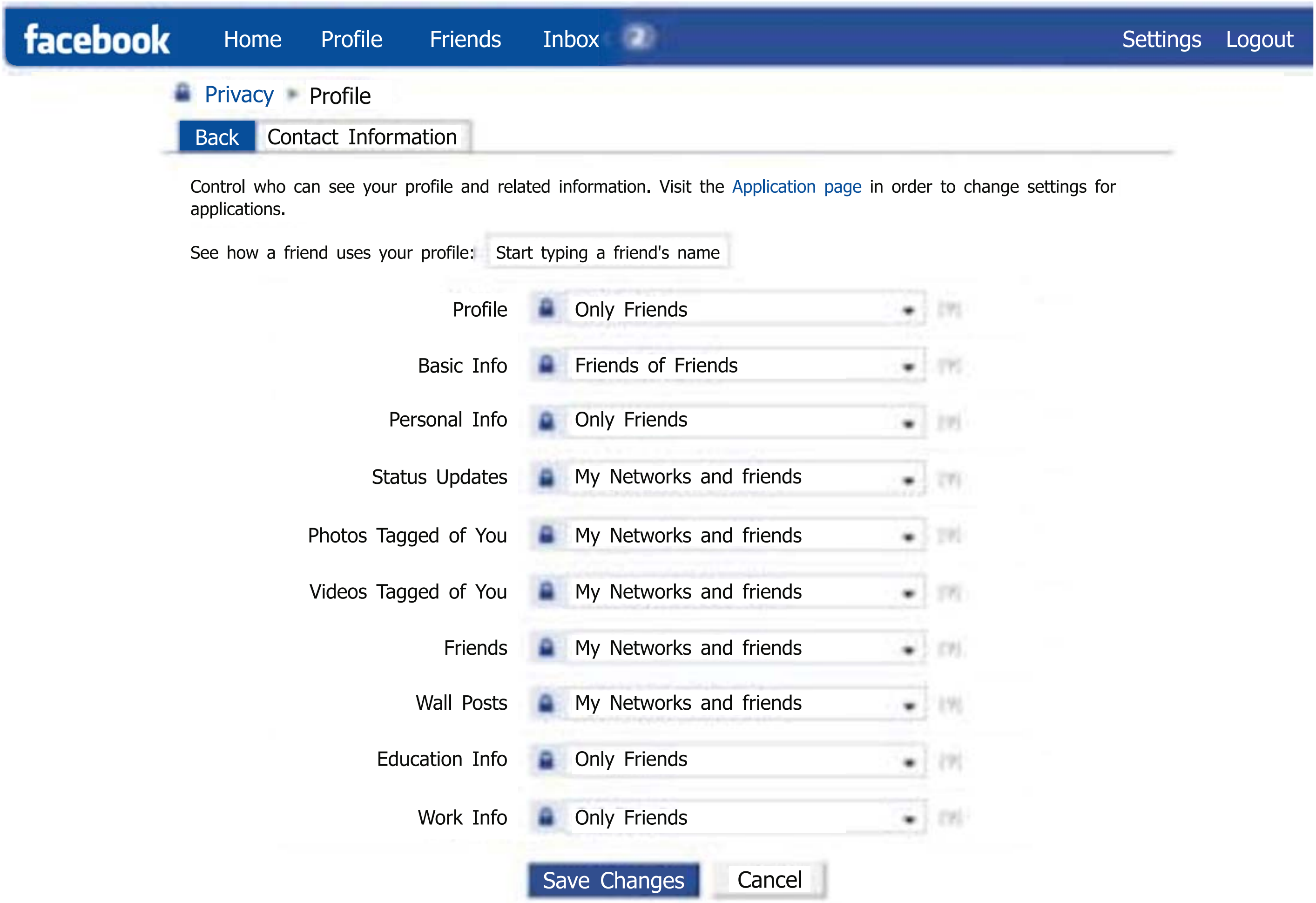
Minimising your online profile will also help reduce the sheer volume of spam that comes your way. We discuss the above scares and precautions in depth below.

Tips for Social Networking Safety

Social networking websites like MySpace, Facebook, Twitter, and Windows Live Spaces are services people can use to connect with others to share information like photos, videos, and personal messages.

As the popularity of these social sites grows, so do the risks of using them. Hackers, spammers, virus writers, identity thieves, and other criminals follow the traffic.

Social networking tools and sites seems to be in direct conflict with another important principle of using the Internet – protect your identity from identity theft. Participating in online social networking sites leaves a trail of personal information that can make stealing your identity a whole lot easier. What's a current-day Internet user to do? Should we go blithely along like a fish protected in a larger school of potential identity theft victims, or maybe we should forego social networking altogether? No and no. Instead each of us should take responsibility for protecting ourselves.



Control who can see your profile and related information. Visit the Application page in order to change settings for applications.

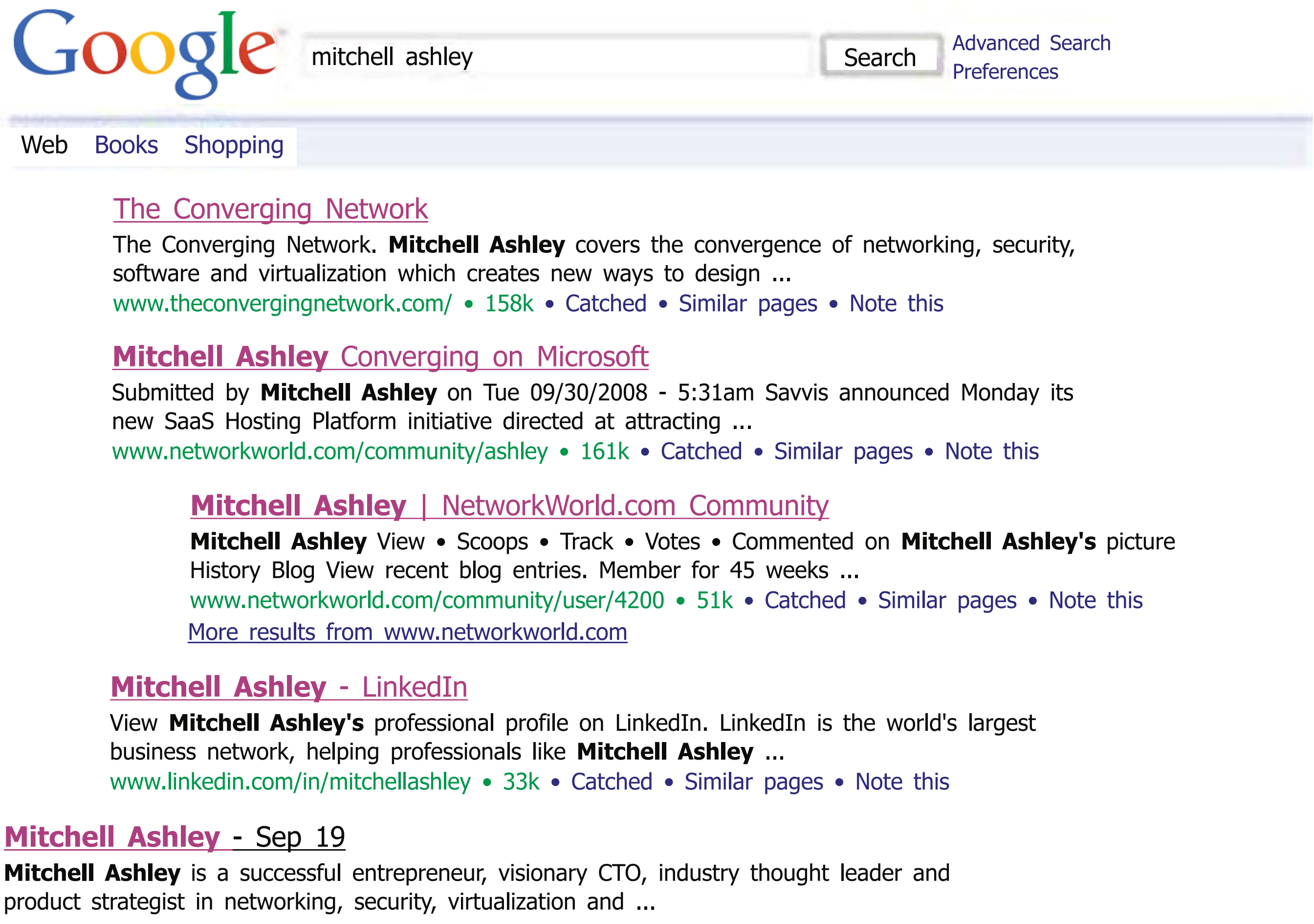
See how a friend uses your profile: Start typing a friend's name

Profile	Only Friends
Basic Info	Friends of Friends
Personal Info	Only Friends
Status Updates	My Networks and friends
Photos Tagged of You	My Networks and friends
Videos Tagged of You	My Networks and friends
Friends	My Networks and friends
Wall Posts	My Networks and friends
Education Info	Only Friends
Work Info	Only Friends

Read these tips to practice safe social networking and help protect yourself when you use social networks.

1. **Use caution when you click links** that you receive in messages from your friends on your social website. Treat links in messages on these sites as you would links in e-mail messages.
2. **Know what you've posted about yourself.Beware of TMI: the five things you should never share:** A common way that hackers break into financial or other accounts is by clicking the “Forgot your password?” link on the account login page. To break into your account, they search for the answers to your security questions, such as your birthday, hometown, high school class, father's middle name, on your social networking site.Social networking means opening up and sharing information online with others, but there's some information you should never share online. Protecting yourself from sharing Too Much Information (TMI) can save you from identity theft and even protect your physical safety. So let's start with the obvious … never share these 5 things...your social security number (including even just the last 4 digits), your birth date, home address or home phone number (although sharing your business phone is ok). Of course, you should protect all of your passwords, PIN numbers, bank account and credit card information. If the site allows, make up your own password questions, and don't draw them from material anyone could find with a quick search.

Also, never share the state where you were born as this information can be used to obtain your social security number and other identity information. Facebook, for example, allows you to restrict who can see your birthday or your hometown (often times the same as your city of birth.) But not every site has these options. In those cases avoid the problem altogether by not entering information you don't want to share. If the sites you are using don't offer these kinds of protections, e-mail them and request these



The Converging Network

The Converging Network. **Mitchell Ashley** covers the convergence of networking, security, software and virtualization which creates new ways to design ...
www.theconvergingnetwork.com/ • 158k • Catched • Similar pages • Note this

Mitchell Ashley Converging on Microsoft

Submitted by **Mitchell Ashley** on Tue 09/30/2008 - 5:31am Savvis announced Monday its new SaaS Hosting Platform initiative directed at attracting ...
www.networkworld.com/community/ashley • 161k • Catched • Similar pages • Note this

Mitchell Ashley | NetworkWorld.com Community

Mitchell Ashley View • Scoops • Track • Votes • Commented on **Mitchell Ashley's** picture History Blog View recent blog entries. Member for 45 weeks ...
www.networkworld.com/community/user/4200 • 51k • Catched • Similar pages • Note this
More results from www.networkworld.com

Mitchell Ashley - LinkedIn

View **Mitchell Ashley's** professional profile on LinkedIn. LinkedIn is the world's largest business network, helping professionals like **Mitchell Ashley** ...
www.linkedin.com/in/mitchellashley • 33k • Catched • Similar pages • Note this

Mitchell Ashley - Sep 19

Mitchell Ashley is a successful entrepreneur, visionary CTO, industry thought leader and product strategist in networking, security, virtualization and ...

features. If enough of us make the request, they'll get the message.

3. **Don't trust that a message really is from whom it says it's from.** Hackers can break into accounts and send messages that look like they're from your friends, but aren't. If you suspect that a message is fraudulent, use an alternate method to contact your friend to find out. This includes invitations to join new social networks.

4. **Customize privacy options**

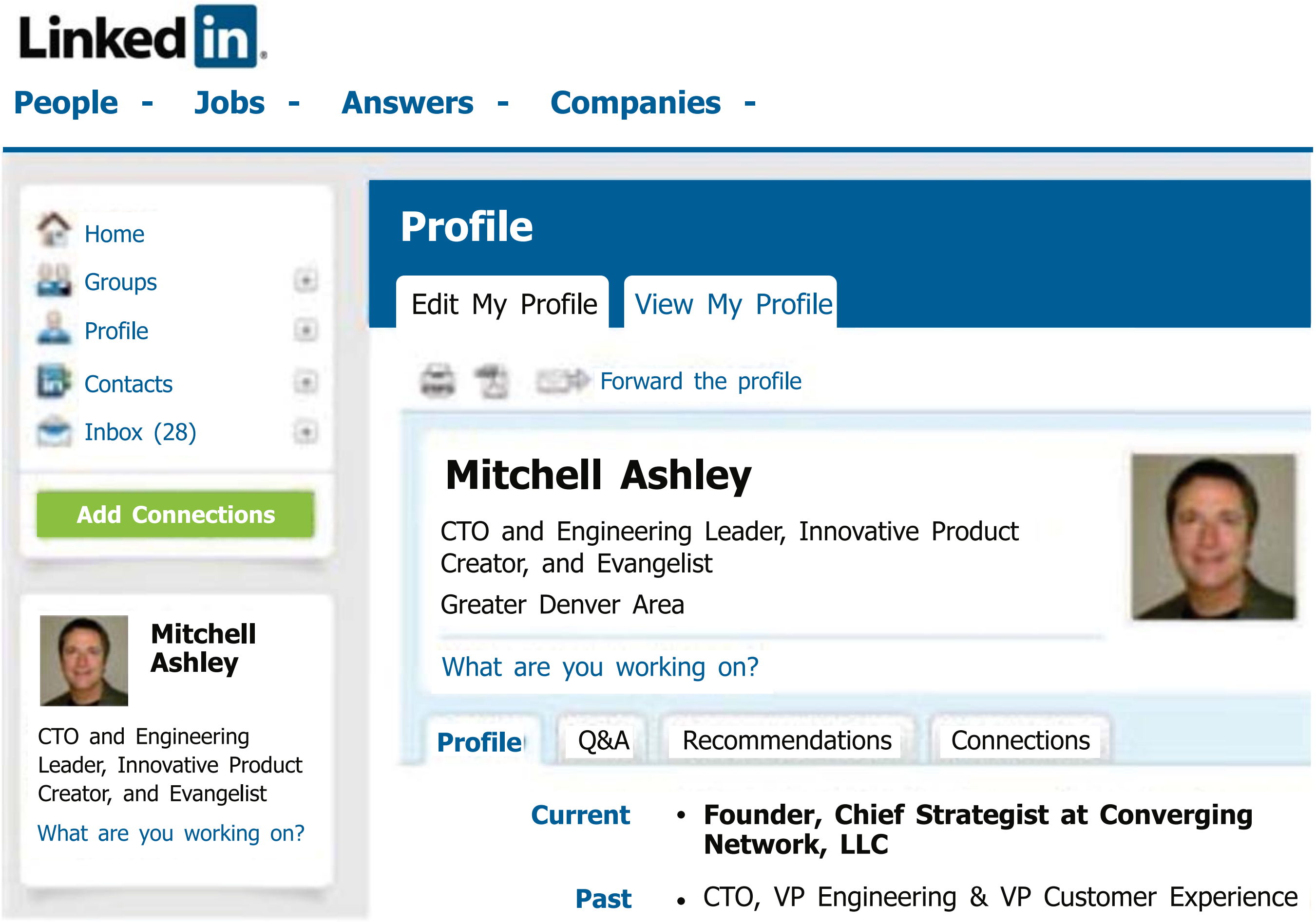
   Social networking sites increasingly give users more control over their own privacy settings. Don't assume you have to take whatever default settings the site gives you. Check out the settings, configuration and privacy sections to see what options you have to limit who and what groups can see various aspects of your personal information. Facebook probably has some of the broadest privacy options, giving you control where no one, friends, friends and networks, or everyone can see basic info, personal info, photos, friends and postings.

   Search is a new area where users are gaining control of what others are allowed to see. Some sites let you set limits on who can see search results about you on the social networking site.

   If you've just joined a social networking site, or even if you have been a user for some time, log onto your account and view and adjust the privacy settings –new settings are often added over time.

5. **To avoid giving away e-mail addresses of your friends, do not allow social networking services to scan your e-mail address book.** When you join a new social network, you might receive an offer to enter your e-mail address and password to find out if your contacts are on the network. The site might use this information to send e-mail messages to everyone in your contact list or even everyone you've ever sent an e-mail message to with that e-mail address. Social networking sites should explain that they're going to do this, but some do not.

6. **Search yourself.** It is a good idea to search your name on Google and check out your profile as others see it on social networking sites. Understand where you show up and what information is available about you, and then adjust your profile, settings and habits appropriately. Don't worry, it's not vain if you only search your own name once a month or so. If you



Mitchell Ashley

CTO and Engineering Leader, Innovative Product Creator, and Evangelist

Greater Denver Area

What are you working on?

Current
- Founder, Chief Strategist at Converging Network, LLC

Past
- CTO, VP Engineering & VP Customer Experience

Mitchell Ashley

CTO and Engineering Leader, Innovative Product Creator, and Evangelist

What are you working on?

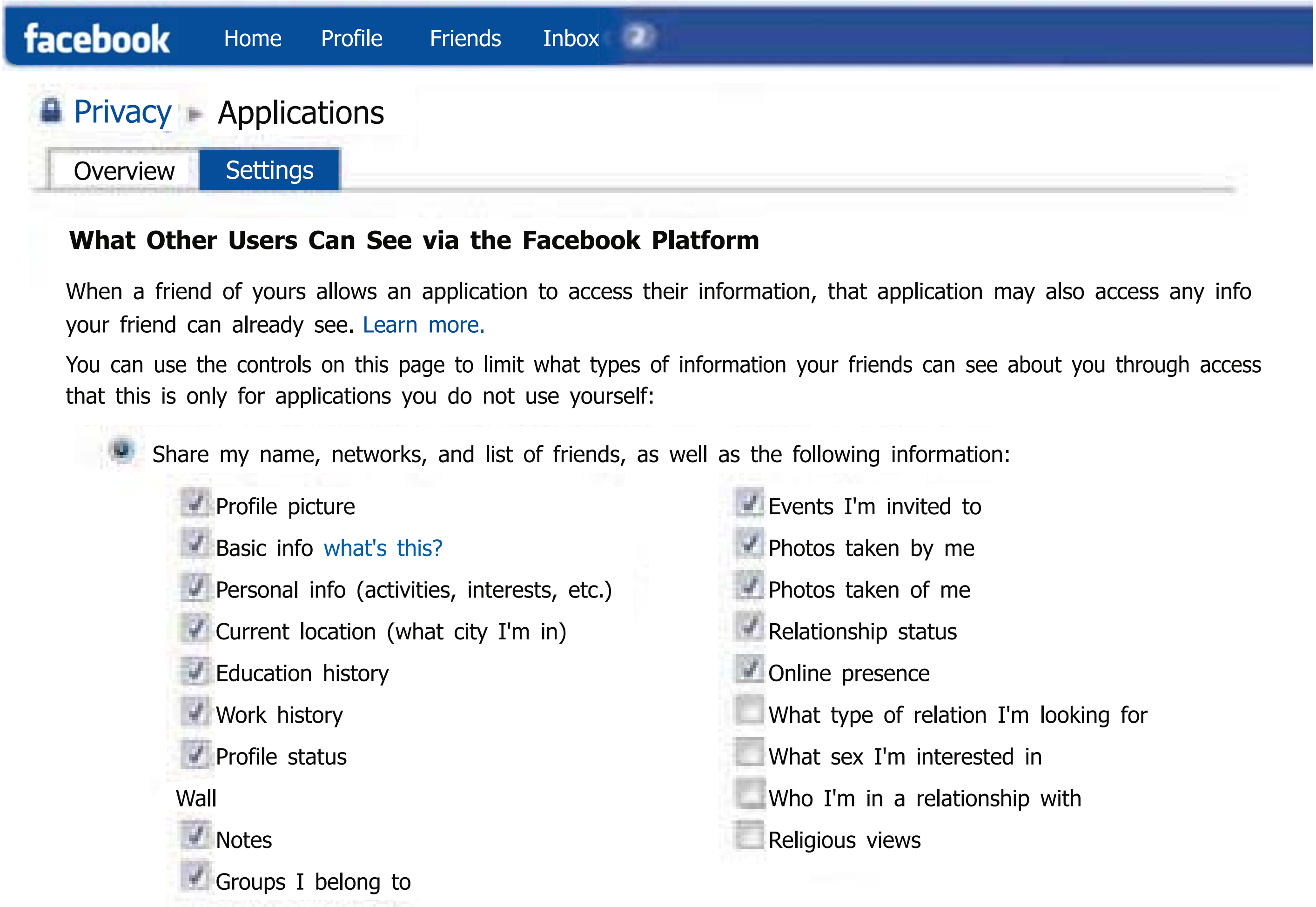
unexpectedly see your name in locations you don't frequent, it could give you a heads up someone else is using your identity online. Set up a Google alert with your name, which emails you when Google finds your name on sites. While some names, like John Smith, are so common they would generate lots of false positives, you may still find out a lot about where your information is appearing online. Even if you find there are others online with the same name, it can help you avoid confusion, (or maybe it's an opportunity to reach out and connect to someone with the same namesake).

7. **Type the address of your social networking site directly into your browser or use your personal bookmarks.** If you click a link to your site through e-mail or another website, you might be entering your account name and password into a fake site where your personal information could be stolen.

8. **Be selective about who you accept as a friend on a social network.Don't trust, just verify.** Identity thieves might create fake profiles in order to get information from you.There are lots of reasons (most of them bad) why someone might impersonate or falsify an identity online. It could be as a prank or for "fun" such as those who impersonate a celebrity as satire. Faking an identity has a legit side too – it can be used by people who simply want to conceal who they are in order to protect their real identities. But its also the first step of those who want to embarrass or defame someone else by impersonating them, or steal an identity for financial gain or other crimes. Two security researchers demonstrated at the Defcon/Black Hat 2008 conference how easy it is to set up a Facebook or LinkedIn site using a false or impersonated identity, including links to malicious sites.

   The question becomes, how can you verify that the page page belongs to who you think it does before sharing too much information or clicking on links? Start by being on the lookout for anything unusual or out of the ordinary. If the content on the site doesn't look like or sound like the person you know, avoid it. E-mail or call your friend to verify the site is legit. Let them know, too, if you think someone else is faking your friend's identity online.

9. **Choose your social network carefully.** Evaluate the site that you plan to use and make sure you understand the privacy policy. Find out if the site



Privacy ► Applications

Overview | Settings

What Other Users Can See via the Facebook Platform

When a friend of yours allows an application to access their information, that application may also access any info your friend can already see. Learn more.

You can use the controls on this page to limit what types of information your friends can see about you through access that this is only for applications you do not use yourself:

● Share my name, networks, and list of friends, as well as the following information:

☑ Profile picture
☑ Basic info what's this?
☑ Personal info (activities, interests, etc.)
☑ Current location (what city I'm in)
☑ Education history
☑ Work history
☑ Profile status
Wall
☑ Notes
☑ Groups I belong to

☑ Events I'm invited to
☑ Photos taken by me
☑ Photos taken of me
☑ Relationship status
☑ Online presence
☐ What type of relation I'm looking for
☐ What sex I'm interested in
☐ Who I'm in a relationship with
☐ Religious views

monitors content that people post. You will be providing personal information to this website, so use the same criteria that you would to select a site where you enter your credit card.

10. **Limit work history details on LinkedIn**

Would you put your full resume online for everyone to see? Probably not. It would be too easy for identity thieves to use the information to fill out a loan application, guess a password security question (like hackers did with VP candidate Sarah Palins' Yahoo account) or social engineer their way into your company's network. Limit your work history details on sites like LinkedIn. If you feel you need the added information to help in a job search, expand the details during the job hunting process and then cut back later after you have a position, leaving just enough information to entice recruiters to contact you with interesting new positions.

LinkedIn also offers some capabilities to restrict information. You can close off access by others to your network of contacts, something you don't have to share if you don't want. This is a common practice by sales professionals and recruiters not wanting to expose their valuable network to others who might poach customers or prospects from them.

11. **Assume that everything you put on a social networking site is permanent.** Even if you can delete your account, anyone on the Internet can easily print photos or text or save images and videos to a computer.

12. **Forget the popularity contest**

Put a number on something and suddenly you have a competition. The person with the most “friends” isn't necessarily the winner in social networking, unless of course you are running for president or you are in some type of recruiting, sales or media business. That's just more people, including possibly strangers, who now have access to more of your information. It is best to only friend people who really are or have become your friends. Your personal information has less opportunity for misuse. If you do get an unsolicited invite to connect, check them out first and try to figure out why you know them or if you even do at all.

For some, blogging and social networking sites are more than casual places for casual connections.

Presidential candidates use MySpace and Facebook to reach out to constituents and hundreds of thousands of potential voters. Industry thought leaders and influencers use blogs and twitter to build up communities of readers and followers for business purposes. That may also be your reason for being a part of online communities, but if your intentions are more casual in nature, massive readership is probably less important to you. Some sites, like Linkedin, discourage blind connections and will begin restricting a user's ability to connect if they receive too many I don't know this person responses. Keeping your network to people you really do know helps keep the spam and other unsolicited messages to a minimum too.

13. **Be careful about installing extras on your site.**

Many social networking sites allow you to download third-party applications that let you do more with your personal page. Criminals sometimes use these applications to steal your personal information. To download and use third-party applications safely, take the same safety precautions that you take with any other program or file you download from the Web.

14. **Avoid accidentally sharing personal details**

You wouldn't put a note on your front door stating, “Away for the weekend… Returning on Monday.” Micro-blogging tools like Twitter and What are you doing right now? features in Facebook, LinkedIn and other social networking sites make it easy to let details slip you wouldn't otherwise tell friends or strangers. Be aware of what information you put out there which others might use for nefarious purposes.

Micro-blogging tool are a bit like the proverbial frog in slowly warming water that's eventually brought to a boil. Over time, seemingly innocuous information can be pieced together, giving lurkers a much more complete and rich picture of you, your family, your habits and other personal information. Software like Twitter is often used at conferences, parties and other social scenes where alcohol is consumed. That makes it even easier for personal details to slip out for the world to see. Twitter users frequently use it to communicate and share their travel woes, giving clue to others that you aren't at home, leaving your family or possessions at risk for intruders. Just keep that in mind as you share tidbits of your life on micro-blogging tools. You might want to be a little bit less specific in your tweets.

15. **Think twice before you use social networking sites at work.Learn how sites can use your information.**

Social network sites are typically free to use which means they are making their money by advertising to you. And that means they are collecting information about you. Is your information shared with outside companies and partners? What information can third-party plug-in software, such as Facebook Applications, use from your profile or page content? Review the site's privacy policy and watch closely the privacy settings you can control.

There is currently a lot of M&A activity in the social networking software industry. A significant part of what an acquirer buys when acquiring a social networking company is the community of users on the site. Your account, including personal information, trades hands from the old company to the new one as part of the transaction. The new owners may have new and different plans for using the information contained in the site. Changes in privacy policies may follow an acquisition. Watch for this when you hear about an acquisition and always read notifications about changes to privacy terms, acceptable use policies and user agreements. ◗

SOURCES / REFERENCES

www.teensafe.com
www.livescience.com
www.pewinternet.org
www.zdnet.com
www.webmd.com
www.networkworld.com
www.pluralsight.com
www.gticanada.com
www.techterms.com
www.internetsociety.org

www.wikipedia.org
www.rasmussen.edu
www.pewinternet.org
www.mozilla.org
www.stickypassword.com
Chris Chase
www.directive.com
Economic Times
The Hindu
Indian Express

Brandon Jones
Vivina Vishwanathan
www.psafe.com
www.ey.com
www.unodc.org
iinet.net.au
resourced.prometheanworld.com
Commonsense.org
nordangliaeducation.com
esafety.gov.au ◗

10 THINGS TO KNOW ABOUT DIGITAL FOOTPRINTS

1 When you search and interact online, a **trail of info** is left behind.

2 Elements of your digital footprints can be **searched or shared.**

3 Digital footprints can be **helpful or harmful** to your reputation both now and in the future.

4 Once online, things can exist **forever** (even if deleted).

5 Always **think** before you post online.

6 Personal information or opinions sent to one person can be **shared** with a larger audience.

7 **Googling yourself** can be a worthwhile exercise.

8 Old or inactive accounts should be **disabled or deleted.**

9 Keep personal details private and control the **privacy settings** on your accounts.

10 Be mindful of the digital footprints of **others** (e.g. Ask before tagging photos).

Internet Safety

The Internet is a huge source of information and means of communication. However, not all of the information or people online are trustworthy.

Safe

S

Ensure personal information and passwords are kept private.

Do not put any of your contact details online and always check your privacy settings on social networking websites.

Never use your real name for your username, and ensure passwords are difficult to guess.

Meet

M

Never meet with an online friend in person, even if you think you know that person well.

Meeting someone from a chat room or social networking website could be dangerous. Online friends are still strangers and may not be who they say they are.

Accept

A

Do not accept emails, instant messages and friend requests from people you do not know.

Messages may contain viruses or unpleasant information and images. Also, remember that 'friends' on social and gaming networks can see and share what you post. Do you want strangers to see everything that you post?

Reliable

R

Not all of the information or people online are reliable. There is a lot of false information.

Always check that the information is correct and use reputable sources. Also, some people post false information or use false identities online to cause harm and trick people.

Try to limit your friends to 'real' friends.

Tell

T

Tell a trusted adult if anything online makes you feel uncomfortable

Many chat rooms and social networking websites have support e-mail addresses or alert buttons that enable users to report inappropriate behaviour, including bullying.

You can log off if you are uncomfortable or suspicious of anything.

CLICK CEOP
Internet Safety

Be careful what you share online!

Anything you post online or send in an e-mail, such as a photo or message, can be copied or shared by anyone who can see it.

Amway™

DIGITAL BHARAT.
DIGITAL AMWAY.
#AbRuknaNahinHai

50,00,000
NEFT transactions
processed to Amway Direct Sellers in a year

ItzCash possibilities unlimited

Partnership with ITZ prepaid cards
Forged a partnership with ITZ prepaid cards six years ago to digitise cash transactions

ATM

ATM enabled purchases
Bank ATMs enrolled for Amway product purchases

95% collections went digital
in November, including 3,00,000 active orders processed via debit, credit, ITZ pre-paid cards & Net Banking

NACH PRODUCT

NACH enabled product purchases
in the North-East

AADHAAR

Mandatory KYC
Bank account and Aadhaar KYC made mandatory for appointment as an Amway Direct Seller

100% digital payments
100% of vendor and employee payments happen digitally

Amway India's state-of-the-art manufacturing facility in Nilakottai, Tamil Nadu.

CUSTOMER SATISFACTION ★ 100% ★ OR MONEY REFUNDED

Join us on facebook@ /amwayindiaofficial or follow us on twitter@ /amwayindia
For more details; please visit us at www.amway.in

Posted at Lodi Road HPO, New Delhi on 9-10th of every month
Published on 6th of every month

RNI No. DELENG/2015/67140
REG. NO. DL (S)–17/3523/2017-19

Printed, published & owned by Bejon Kumar Misra, Printed at M/s. Swastika Creation, 19, D.S.I.D.C. Shed, Scheme 3,
Okhla Phase II, New Delhi - 110020 and Published at B - 306, 1st Floor, C.R. Park, New Delhi-110019,
Editor: Bejon Kumar Misra