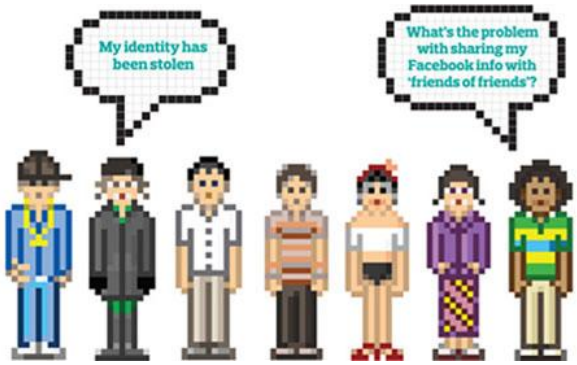
20 ways to keep your Internet identity safe from hackers

James Silver
The Observer, Sunday 12 May 2013

Do you use the same password for all websites? Do you over share on Facebook? If so, you're a target for cybercriminals – whose computer scams are costing Britain £27bn a year? We asked experts for their top tips to beat the fraudsters.



Cybercrime costs Britain £27 billion a year: don't make it easy for the fraudsters. We're high up in the Gherkin in the City of London and Garry Sidaway, director of security strategy at Integralis, a firm which advises government agencies, pharmaceutical and financial services multinationals, is giving my computer a security MOT. "You don't have anti-virus software, I see," he says, a trace of mockery in his voice. "That's your first mistake."

According to Sidaway, while most of us are much more aware of the risks now ("My mum shreds her documents even if she doesn't know why," he says), we should all be raising the bar. He thinks we Britons are an overly trusting lot. Sitting ducks for an armada of hackers, who are every bit as focused on stealing our data as we are relaxed about storing it. "The criminal gangs know exactly which kind of data they want and where it is likely to be," he explains. "Conversely we're not sure what they're after."

So what are they after, I ask? "We are seeing a wide variety of attacks – everything from opportunists trying to extract passwords through phishing [emails which purport to be from legitimate sources and attempt to get us to click on an infected link] to highly organised crime units targeting businesses and government systems in an effort to steal intellectual property and information related to critical infrastructure."

The government estimates that the total cost of cybercrime in the UK is £27bn a year. The majority (£21bn) is committed against businesses, which face

high levels of intellectual property theft and industrial espionage.

Enabled by the sharing culture on social media – and with ever more sophisticated malicious software known as malware at their disposal – cybercriminals have become far more adept at crafting attacks and targeting individuals and organisations. Phishing emails purporting to be from friends, often reflecting our interests – perhaps gleaned from social media sites – or from trusted organisations such as your bank or HM Revenue & Customs encourage us to click on infected links or attachments containing malware. (A recent example of the latter was malware disguised as a security warning from Microsoft's digital crimes unit.) "We have a level of trust in certain organisations and criminals exploit that trust," says Sidaway.

Typically, these so-called "man-in-the-middle" attacks install colourfully named Trojans (pieces of malware, essentially) such as Zeus, SpyEye or Citadel on computers, which have the effect of compromising, for example, online banking transactions. "Everything you then do on your compromised laptop is subverted through a hacking site which means when you [communicate] with your bank, you are going through a man in the middle. Initially, man-in-the-middle attacks were passwords used in authentication – the criminal would wait until you had finished to start using the credentials they'd just gathered. This is why banks brought in one-time passwords or codes," he says.

"But more recent malware will perform a man-in-the-middle attack to obtain the user's session (a session is created after a user logs in successfully and the browser and the bank's website use this to continue the interaction) and fake the logout requests. Once the user thinks they've logged out, the attacker can make payments using the existing session without the victim seeing any changes to their balance until the next time they log on. This is partly why banks have rolled out card readers to help prevent payments to new payees." He adds: "It's a constant game of cat and mouse."

TWENTY COMMANDMENTS: THE DOS AND DON'TS OF ONLINE SAFETY

1. **Never click on a link you did not expect to receive**

   The golden rule. The main way criminals infect PCs with malware is by luring users to click on a link or open an attachment. "Sometimes phishing emails contain obvious spelling mistakes and poor grammar and are easy to spot," says Sidaway of Integralis. "However, targeted attacks and well-executed mass mailings can be almost indistinguishable [from genuine emails]." Social media has helped criminals profile individuals, allowing them to be much more easily targeted, he adds. "They can see what you're interested in or what you [post] about and send you crafted messages, inviting you to click on something. Don't."

2. **Use different passwords on different sites**

   With individuals typically having anything up to 100 online accounts, the tendency has become to share one or two passwords across accounts or use very simple ones, such as loved ones' names, first pets or favourite sports teams. Indeed, research by Ofcom last month revealed that over half of UK adults (55%) use the same passwords for most, if not all, websites they visit, while one in four (26%) use birthdays or names as passwords. Any word found in the dictionary is easily crackable. Instead, says Sian John, online security consultant at Symantec, have one memorable phrase or a line from a favourite song or poem. For example: "The *Observer* is a Sunday newspaper" becomes "toiasn". Add numerals and a special character thus: "T0!asn". Now for every site you log on to, add the first and last letter of that site to the start and end of the phrase, so the password for Amazon would be "AT0!asnn". At first glance, unguessable. But for you, still memorable."

3. **Never reuse your main email password**

   A hacker who has cracked your main email password has the keys to your [virtual] kingdom. Passwords from the other sites you visit can be reset via your main email account. A criminal can trawl through your emails and find a treasure trove of personal data: from banking to passport details, including your date of birth, all of which enables ID fraud. Identity theft is estimated to cost the UK almost £2bn a year.

4. **Use anti-virus software**

   German security institute AV-Test found that in 2010 there were 49m new strains of malware, meaning that anti-virus software manufacturers are engaged in constant game of "whack-a-mole". Sometimes their reaction times are slow – US security firm Imperva tested 40 anti-virus packages and found that the initial detection rate of a new virus was only 5%. Much like flu viruses and vaccine design, it takes the software designers a while to catch up with the hackers. Last year AV-Test published the results of a 22-month study of 27 different anti-virus suites and top-scoring packages were Bitdefender, Kaspersky and F-Secure. Meanwhile, security expert Brian Krebs published the results of a study of 42 packages which showed on average a 25% detection rate of malware – so they are not the entire

answer, just a useful part of it.

5. **If in doubt, block**
   Just say no to social media invitations (such as Facebook-friend or LinkedIn connection requests) from people you don't know. It's the cyber equivalent of inviting the twitchy guy who looks at you at the bus stop into your home.

6. **Think before you tweet and how you share information**
   Again, the principal risk is ID fraud. Trawling for personal details is the modern day equivalent of "dumpster-diving", in which strong-stomached thieves would trawl through bins searching for personal documents, says Symantec's John. "Many of the same people who have learned to shred documents like bank statements will happily post the same information on social media. Once that information is out there, you don't necessarily have control of how other people use it." She suggests a basic rule: "If you aren't willing to stand at Hyde Park Corner and say it, don't put it on social media."

7. **If you have a "wipe your phone" feature, you should set it up**
   Features such as Find My iPhone, Android Lost or BlackBerry Protect allow you to remotely to erase all your personal data, should your device be lost or stolen. "Absolutely, set it up," advises Derek Halliday of mobile security specialist Lookout. "In the case where your phone is gone for good, having a wipe feature can protect your information from falling into the wrong hands. Even if you didn't have the foresight to sign up, many wipe your phone features can be implemented after the fact."

8. **Only shop online on secure sites**
   Before entering your card details, always ensure that the locked padlock or unbroken key symbol is showing in your browser, cautions industry advisory body Financial Fraud Action UK. Additionally the beginning of the online retailer's internet address will change from "http" to "https" to indicate a connection is secure. Be wary of sites that change back to http once you've logged on.

9. **Don't assume banks will pay you back**
   Banks must refund a customer if he or she has been the victim of fraud, unless they can prove that the customer has acted "fraudulently" or been "grossly negligent". Yet as with any case of fraud, the matter is always determined on an individual basis. "Anecdotally, a customer who has been a victim of a phishing scam by unwittingly providing a fraudster with their account details and passwords only to be later defrauded could be refunded," explains Michelle Whiteman, spokesperson for the Payments Council, an industry body. "However, were they to fall victim to the same fraud in the future, after their bank had educated them about how to stay safe, it is possible a subsequent refund won't be so straightforward. Under payment services regulations, the onus is on the payment-service provider to prove that

the customer was negligent, not vice versa. Credit card protection is provided under the Consumer Credit Act and offers similar protection."

10. Ignore pop-ups

Pop-ups can contain malicious software which can trick a user into verifying something. "[But if and when you do], a download will be performed in the background, which will install malware," says Sidaway. "This is known as a drive-by download. Always ignore pop-ups offering things like site surveys on e-commerce sites, as they are sometimes where the malcode is."

11. Be wary of public Wi-Fi

Most Wi-Fi hotspots do not encrypt information and once a piece of data leaves your device headed for a web destination, it is "in the clear" as it transfers through the air on the wireless network, says Symantec's Sian John. "That means any 'packet sniffer' [a program which can intercept data] or malicious individual who is sitting in a public destination with a piece of software that searches for data being transferred on a Wi-Fi network can intercept your unencrypted data. If you choose to bank online on public Wi-Fi, that's very sensitive data you are transferring. We advise either using encryption [software], or only using public Wi-Fi for data which you're happy to be public – and that shouldn't include social network passwords."

12. Run more than one email account

Thinking about having one for your bank and other financial accounts, another for shopping and one for social networks. If one account is hacked, you won't find everything compromised. And it helps you spot phishing emails, because if an email appears in your shopping account purporting to come from your bank, for example, you'll immediately know it's a fake.

13. Macs are as vulnerable as PCs

Make no mistake, your shiny new MacBook Air can be attacked too. It's true that Macs used to be less of a target, simply because criminals used to go after the largest number of users – ie Windows – but this is changing. "Apple and Microsoft have both added a number of security features which have significantly increased the effectiveness of security on their software," says Sidaway, "but determined attackers are still able to find new ways to exploit users on almost any platform."

14. **Don't store your card details on websites**

    Err on the side of caution when asked if you want to store your credit card details for future use. Mass data security breaches (where credit card details are stolen en masse) aren't common, but why take the risk? The extra 90 seconds it takes to key in your details each time is a small price to pay.

15. **Add a DNS service to protect other devices**

    A DNS or domain name system service converts a web address (a series of letters) into a machine-readable IP address (a series of numbers). You're probably using your ISP's DNS service by default, but you can opt to subscribe to a service such as OpenDNS or Norton ConnectSafe, which redirect you if you attempt to access a malicious site, says Sian John. "This is helpful for providing some security (and parental control) across all the devices in your home including tablets, TVs and games consoles that do not support security software. But they shouldn't be relied upon as the only line of defence, as they can easily be bypassed."

16. **Enable two-step verification**

    If your email or cloud service offers it – Gmail, Dropbox, Apple and Facebook do – take the trouble to set this up. In addition to entering your password, you are also asked to enter a verification code sent via SMS to your phone. In the case of Gmail you only have to enter a fresh code every 30 days or when you log on from a different computer or device. So a hacker might crack your password, but without the unique and temporary verification code should not be able to access your account.

17. **Lock your phone and tablet devices**

    Keep it locked, just as you would your front door. Keying in a password or code 40-plus times a day might seem like a hassle but, says Lookout's Derek Halliday, "It's your first line of defence." Next-generation devices, however, are set to employ fingerprint scanning technology as additional security.

18. **Be careful on auction sites**

    On these sites in particular, says Symantec's Sian John, exercise vigilance. "Check the seller feedback and if a deal looks too good then it may well be," she says. "Keep your online payment accounts secure by regularly changing your passwords, checking the bank account to which it is linked and consider having a separate bank account or credit card for use on them, to limit any potential fraud still further."

19. **Lock down your Facebook account**

    Facebook regularly updates its timeline and privacy settings, so it is wise

to monitor your profile, particularly if the design of Facebook has changed. Firstly, in the privacy settings menu, under "who can see my stuff?" change this to "friends" (be warned: setting this to "friends of friends" means that, according to one Pew study, on average you are sharing information with 156,569 people). Also in privacy, setting "limit old posts" applies friends-only sharing to past as well as future posts. Thirdly, disable the ability of other search engines to link to your timeline.

You should also review the activity log, which shows your entire history of posts and allows you to check who can see them. Similarly, you should look at your photo albums and check you're happy with the sharing settings for each album. In the future you may want to consider building "lists" – subsets of friends, such as close friends and family, who you might want to share toddler photographs with, rather than every Tom, Dick and Harriet.

Also, remove your home address, phone number, date of birth and any other information that could used to fake your identity. Similarly you might want to delete or edit your "likes" and "groups" – the more hackers know about you, the more convincing a phishing email they can spam you with. Facebook apps often share your data, so delete any you don't use or don't remember installing. Finally, use the "view as" tool to check what the public or even a particular individual can see on your profile, continue to "edit" and adjust to taste. If this all sounds rather tedious, you just might prefer to permanently delete your account.

20. **Remember you're human after all**

While much of the above are technical solutions to prevent you being hacked and scammed, hacking done well is really the skill of tricking human beings, not computers, by preying on their gullibility, taking advantage of our trust, greed or altruistic impulses. Human error is still the most likely reason why you'll get hacked.