

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. 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. 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. One in four people in the UK 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: "Mary had a little lamb" becomes "mhall". Add numerals, a capital and punctuation thus: "Mha11!" (use the numeral 1 in place of the letter l). 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 "Amha11!n". At first glance, unguessable. Different for different sites. 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.

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%. 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 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.

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. “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.” A basic rule: “If you aren’t willing to stand in a crowded place and say it, don’t put it on social media.”

7. If you have a “wipe your phone” feature — use it

Features such as Find My iPhone, Android Lost or BlackBerry Protect allow you to remotely erase all your personal data, should your device be lost or stolen. 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. 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, the matter is always determined on an individual basis.

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. 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 wifi

Most wifi 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. “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 wifi network, can intercept your unencrypted data. If you choose to bank online on public wifi, that’s very sensitive data you are transferring. We advise either using encryption [software], or only using public wifi 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 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, 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?

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. 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. 1. 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). 2. Also in privacy, setting "limit old posts" applies friends-only sharing to past as well as future posts. 3. Disable the ability of other search engines to link to your timeline. 4. Review the activity log, which shows your entire history of posts and allows you to check who can see them. 5. Remove your home address, phone number, date of birth and other information that could be used to fake your identity. 6. Delete or edit your "likes" and "groups" — the more hackers know about you, the more convincing a phishing email they can spam you with. 7. Facebook apps often share your data, so delete any you don't use or don't remember installing. 8. 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.

20. Remember you're human after all

While much of the above prevents you being hacked, hacking done well is really the skill of tricking humans, not computers, by preying on their gullibility. Human error is still the most likely reason why you'll get hacked.