Don't Get Hacked in 2019

Cyber-criminals are coming up with ever more ingenious ways to infect your PC and steal your data. **Will Stapley** reveals the top new threats and how to avoid them

Fake online chatbots

Chatbots are used by many companies these days to provide automated answers to basic customer queries. However, security company WatchGuard (www.snipca.com/30082) has warned that in 2019 fake chatbot windows could be inserted into hacked websites, including online banking services. Using advanced artificial intelligence (AI), it's feared these could fool people into providing personal information (such as passwords or account numbers), or may offer links to dangerous websites and downloads.

Protect yourself: Be sceptical when using any form of online chat. Most official websites never ask for personal information. If you suspect something is wrong, close the chat window and contact the company by phone instead.

Phishing emails get personal

This year, phishing emails will become much harder to spot – and it's all down to the rise in data breaches. The sheer wealth of leaked personal data that's now available on the dark web will allow hackers to create even more personalised phishing emails.

Imagine, for example, receiving an email that purports to be from your favourite online store. It lists your recent purchases, and includes your home address and other personal details. At the bottom of the email, there's a voucher offer. All you need to do is click on the link – and the hacker's work is done.

Protect yourself: The threat is so serious, the National Cyber Security Centre (part of GCHQ) has issued guidance at www.snipca.com/30083. This includes using HaveIBeenPwned? (https://haveibeenpwned.com), a free website that notifies you if your personal details (email address, passwords or home address) have been leaked by a breach. Click 'Notify me' at the top to register your email (see screenshot below).

Fileless vaporworms emerge

In contrast to traditional viruses, which attach themselves to files, fileless malware resides only in your computer's memory. Because it doesn't infect files, it's much harder for antivirus programs to detect. And this year, fileless malware is set to become a bigger threat by taking on worm-like properties, meaning they can spread faster by self-replicating (Watchguard calls these 'vaporworms' – www.snipca.com/30084). Once your computer is infected, hackers can use it to send out spam or take part in denial-of service attacks and more.

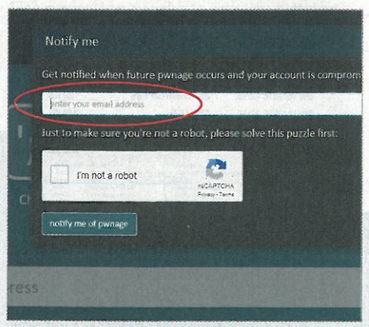
Protect yourself: Vaporworms infect PCs through macros in documents and spreadsheets. Popular office suites, such as Microsoft Office and LibreOffice will warn you before running a macro. If you're not entirely sure where a particular document or spreadsheet has come from, we recommend you don't run the macro.

Dangerous sites flagged as secure

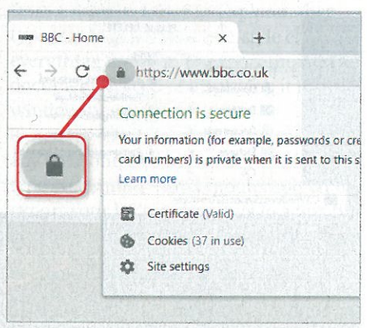
That comforting padlock icon in your browser's address bar, which indicates your connection to the current site is encrypted using HTTPS (see screenshot below left), might not be so reliable after all.

According to a report by PhishLabs (www.snipca.com/30093), by the end of 2018 nearly half of all phishing sites were using HTTPS, meaning they too displayed the padlock icon. This figure is up 25 per cent on 2017, indicating that the problem is only likely to get worse in 2019.

Protect yourself: Make sure you enter personal data only on sites displaying the padlock symbol, but even then don't assume it means the site is safe or genuine. It's a good idea to use VirusTotal's URL scanner (www.snipca.com/30128) to see whether the website is listed as potentially dangerous.



Get notifications from HaveIBeenPwned? when your details have been leaked in a data breach



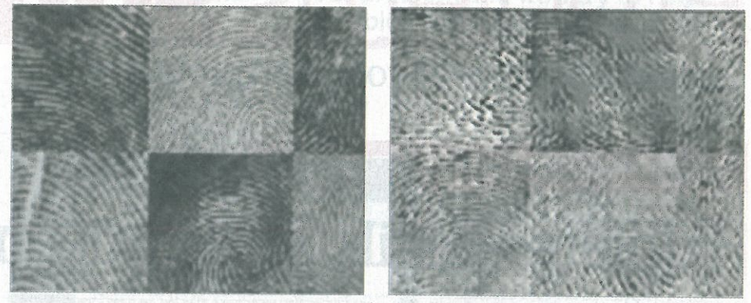
The padlock means your connection to a site is secure, but not that the website itself is safe

Hackers target smart devices

Researchers at Indiana University in the US have warned of a new smart-speaker threat called 'voice squatting', which takes advantage of users mispronouncing app names. To demonstrate it, the team created a fake Amazon Echo app called Rap Game and showed how it could be unwittingly installed by people asking to load the genuine (and similar-sounding) Rat Game app. You can watch how easily the fake app can be installed (and read responses from smart-speaker manufacturers Google and Amazon) at www.snipca.com/30085.

The researchers say they're working with both companies to help improve the detection of malicious apps that use voice-squatting techniques, but it highlights the vulnerabilities of a system designed to be purely voice controlled.

Protect yourself: Use your smart speaker's app to periodically check which third-party apps you have installed. If you don't recognise something, remove it immediately.



Real fingerprints (left) and their AI-generated versions (right), as revealed by NYU research

Biometric weaknesses exposed

Biometric security that uses your fingerprint, eyes or entire face to unlock a device is often considered nigh-on unhackable. However, consumer credit agency Experian's 2019 Data Breach Industry Forecast (www.snipca.com/30086) predicts major flaws will be exposed this year.

These claims are backed up by a New York University (NYU) study carried out last year, which demonstrated how criminals can use artificial intelligence to generate 'master key' fingerprints that contain common fingerprint patterns. The study showed how a single master key print can mimic the real fingerprints of more than one person (see screenshot above), much like a skeleton key mimics a real key. While techniques such as this are likely to be used against businesses rather than home users, it highlights that biometric security may not be as secure as we've been led to believe.

Protect yourself: Don't rely solely on biometric verification, and use two-factor authentication on any service that offers it.

Kids' tech becomes a target

Last year, a flaw was discovered in two of VTech's tablets aimed at children (the InnoTab Max and Storio Max), which hackers could have exploited to spy on kids via the built-in webcam. VTech issued a firmware update, but owners need to update it manually to fix the vulnerability (see www.snipca.com/30088).

It's a handy reminder that, while we're used to our Windows PCs automatically installing important security fixes, more niche devices often need to be updated manually.

Protect yourself: Don't assume tech aimed at kids is inherently safe. Regularly check all childrens' devices you have for security updates.

Sextortion with ransomware

Sextortion emails - where criminals try to blackmail you by claiming they have footage of you watching porn sites - are on the rise. And this year, the emails are getting even more sinister. Security firm ProofPoint (www.snipca.com/30090) recently spotted a new variant that now also infects your PC with ransomware if you click a link that promises to show evidence of the 'material' the blackmailers have on you.

Protect yourself: Never click on links in suspicious emails and keep a copy of your PC backups on an external hard drive that's disconnected from your PC when not in use. ca

UK hit by Sharpshooter malware

Most security firms agree that attacks from hackers backed by nation states are only likely to increase this year. The latest high-profile attack (called Operation Sharpshooter), which took place across October and November 2018, targeted the computers of 87 nuclear, defence, energy and financial organisations across the world, infecting them with a virus, according to McAfee (www.snipca.com/30112). Most of the attacks took place in English-speaking countries (including the UK) - and all the signs are that they were state sponsored, most likely by North Korea.

It appears Sharpshooter was intended to gather data stored on the infected computers, rather than stop them working, or damage infrastructure. It's feared this data could pave the way for a more serious attack this year, which may bring down vital services.

The most surprising thing is that the virus was spread using an infected macro within a Microsoft Word document! It's a timely reminder that for all the cutting-edge methods employed by hackers, sometimes it's the basic, old-fashioned methods that remain chillingly effective. The ease with which the virus spread is likely to encourage similar attacks this year.