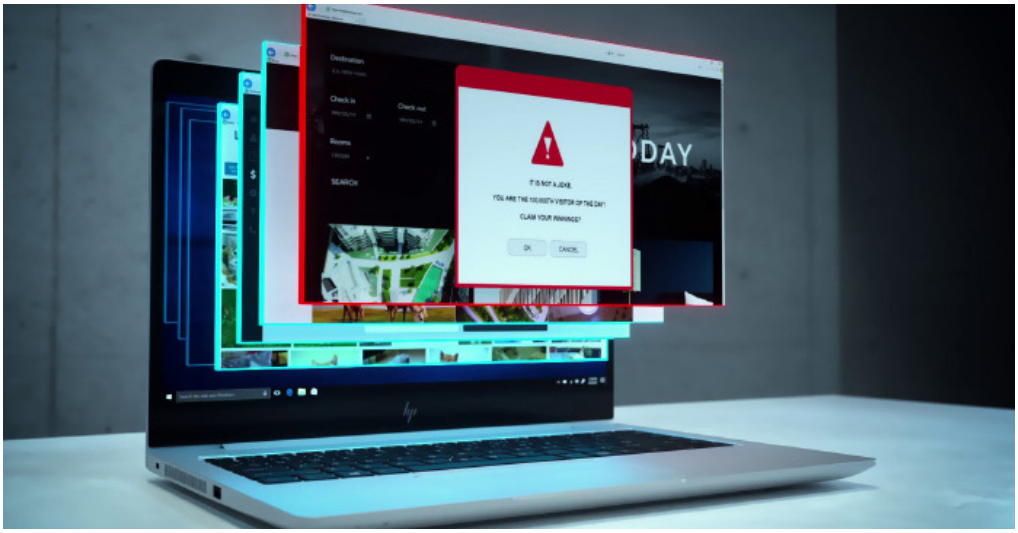
Phishing isn't just for emails anymore

Soukaina El Idrissi

Learn more



A web browser is a portal into a world of information...and threats. So, what can you do about it to protect your business?

Web browsers have a lot to answer for. In a recent survey of 400 CIOs, 68% said that cyber criminals are now so sophisticated, their staff struggle to differentiate between safe and unsafe sites[1]. With that in mind, it's no surprise that 70% of IT professionals experience weekly phishing attacks – and not just via email[2]. Sophisticated hackers are now using social media, advertisements, and common website misspellings to trick employees into revealing sensitive personal information. As phishing scams become increasingly difficult to recognise, businesses are struggling to protect their workforce from these attacks.

Despite greater awareness and investment in security software and employee education, there's been a 232% jump in cyber-attacks on notebooks and desktops over the last six years[3]. Cyber-criminals are still getting through, because the numbers are on their side. It takes a huge amount of effort to safeguard data, but it only takes one employee clicking on one malicious link to bring down your business.

Social media cyber-attacks are a large part of this problem. Platforms, like Facebook and Twitter, are rich hunting ground for cybercriminals. Not only are they designed for engagement and communication, they're also simple to use and cheap to run. It's incredibly easy to set up fraudulent accounts and start posting malicious content, from links and data harvesting to landing pages with unreliable pop-ups.

Most of these online activities are based on phishing techniques, which used to be reserved to email. Social media enables connections between people, and it doesn't take much to build up a substantial, credible persona and following with genuine users of the platforms.

Vevo, the streaming service, was the recent victim of a massive data breach. One of its employees was targeted by a LinkedIn phishing scam, which led to 3.12TB worth of internal files being leaked online. This included, videos, office documents, promotional material, yet to be used social media content, and information about recording artists signed to the participating record companies[4].

Hacking squad OurMine claimed responsibility for the attack, after an altercation over email with a member of staff at Vevo. This shows the danger of **spear-phishing**, a targeted attack that tries to steal specific details from a specific target. Most often hackers disguise themselves as a friend or trusted source (i.e. your bank) to trick the target into releasing information – which accounts for 91% of attacks.

Phishing isn't just for emails anymore

For most businesses that fall victim to a phishing attack, like Vevo's, the consequences can be both damaging and longstanding. Not only can they result in the loss of employee productivity and customer data, but in the loss of customers themselves. The trust your customers have in your business could take a huge hit due to a security breach – to them, you're no longer a trustworthy holder of information. And, although this can be salvaged, more often, the implications are permanent.

In Q4 2017, social media phishing attacks spiked to 500%, with a trend for fake accounts posing as customer support for big name brands[5]. This development became known as **angler-phishing**, because hackers set bait and wait for social media users to come to them. By using the same branding and an authentic looking account name, the millions of people who rely on web-based social media are often fooled by a convincing attack. Then, as soon as a user engages, the fake account sends them a link to a phishing site and asks them to log in, allowing the phisher to reach the ultimate goal of obtaining private data.

One of the easiest ways to prevent your employees from engaging phishing via social media is to instigate behavioural change at work. It should help your staff to avoid making the kind of simple mistakes that lead to devastating consequence for your business:

1. Limit interactions to users you can trust
2. Don't click through links from an unverified source
3. Never download file attachments from social media
4. Enable two-factor authentication on all social media accounts and devices – it'll make it harder to hack them
5. Give extra training to employees with high-access privileges or social-facing roles

Another essential aspect of your security plan to look at is the technology you're using to stay cyber resilient. The HP Elite family, for example, is a of laptops and PCs have been designed with security from the ground up.

One of these features is HP Sure Click, available on select HP Elite platforms, which approaches secure browsing differently. Instead of just flagging dangerous sites for users to avoid, it also keeps malware, ransomware and viruses from infecting other browser tabs and the wider system. When a user starts a browsing session, every site visited triggers HP Sure Click. For example, each time a website is visited, HP Sure Click creates a hardware-based isolated browsing session, which eliminates the ability of one website from infecting other tabs or the system itself.

When it comes to businesses changing their security strategy and getting hold of these cutting-edge devices, like the HP EliteBook 800 Series, with optional 8th Generation Intel® Core™ Processors, it can feel easier said than done. That's where a solution like HP Device as a Service (DaaS) comes in. It's a modern PC consumption model that simplifies how commercial organisations equip their employees with the right hardware and accessories, manage multi-OS device fleets, and get additional lifecycle services. HP DaaS offers simple, yet flexible plans, at one price per device to keep everything running smoothly and efficiently.

Ultimately, having a well-trained team and devices that are optimised for security will help you combat social media cybercrime, one of the top cyber threats out there. It's only going to get bigger and more sinister, so now is the time to upscale your defences.

Discover the benefits of HP security solutions to your business.

Sources:

1. https://www.bromium.com/company/press-releases/majority-cios-believe-they-are-losing-battle-against-cybercrime.html
2. https://www.engineering.com/DesignerEdge/DesignerEdgeArticles/ArticleID/8355/HP-Nearly-70-of-IT-Professionals-Experience-Weekly-Phishing-Attacks.aspx
3. http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/
4. https://www.zerofox.com/blog/vevo-hacked-via-linkedin-phishing-campaign/
5. https://www.infosecurity-magazine.com/news/social-media-phishing-attacks-soar/

4AA7-3218EEE, May 2018