+44 345 094 0945
www.waterstons.com

Article

Dec 2021

What is social media phishing and how can it affect you and your business?

With over 1.3 billion users a day, social media is becoming a favourite target for many hackers. We are often made aware of scams through email, text, and phone calls but many people are less aware of attacks through social media platforms, known as social media phishing.

What is social media phishing?

Social media phishing is any attack that happens through social media platforms such as Instagram, LinkedIn, Facebook, or Twitter. The reason behind social media attacks is often to steal personal data or gain control of your social media account, to carry out further phishing attacks against your friends, colleagues, or if you use these platforms for business, your customers too.

With over 90% of user's accessing social media via mobile devices, social media phishing has also been linked to mobile phishing, already a significant issue for businesses. A recent study by Lookout found that the rate at which enterprise users are falling for mobile phishing attacks has increased on average 85% year on year from 2011 to 2018. This worrying trend means that social media phishing should be a priority for businesses in 2022.

How does social media phishing affect businesses?

According to PhishLabs, at the start of 2021, the average business experienced 34 phishing attacks on social media per month, which then rose by around 47% to 50 per month only six months later. The most common type of social media attack was fraud-related closely followed by employee, brand and executive impersonations.

Social media phishing attacks can cause havoc to businesses and customers. Any size breach usually leads to some form of business disruption, generally in the form of loss of data or assets, or, if the phishing attack affects your customers, they may begin to lose confidence in your brand, which can result in the loss of custom. If your customers' data gets stolen or leaked it can also result in lawsuits and fines, especially if the data is covered by data protection regulations.

Some of the most popular apps in the world, WhatsApp and Facebook messenger are also among the riskiest apps for business users. Appthority's report in 2018 (based on scans of its enterprise customers mobile devices) found that WhatsApp and Facebook Messenger had the highest risk score. Companies were not only concerned with traditional data leakage but also leaking contact lists and in some cases employee locations.

According to the 2018 Mobile Phishing Report by Wandera, employees are 18x more likely to fall for mobile phishing attacks than download mobile malware.

Why are social media phishing attacks successful?

While most phishing still occurs via email this is quickly changing, since social media phishing attacks are much more successful than traditional email phishing. A study by Google found that email phishing is on average 13.7% effective. In contrast, a later study by Blackhat found that social media phishing attacks were up to 66% effective.

Here are some examples of why social media phishing attacks are successful:

Shortened URLs - With URLs often being shortened in mobile browsers it is harder to detect illegitimate sites based on a glance at the URL – a common technique for spotting phishing. It is also harder to examine URLs before clicking them in some social media apps, such as Facebook Messenger since generally, it does not preview the full URL, just the hyperlinked text.

Message Forwarding - Often WhatsApp scams use message forwarding as a way of sending a malicious message through a trusted network. Only one person needs to forward it before it appears to be coming from a legitimate source. For example, one phishing attack involved a message telling users that WhatsApp was creating a 'Gold' service. The link in the message led users to a malicious website, however, the scam still spread across the social network, generally via large group chats.

Public Accounts / Visible Accounts - LinkedIn attacks operate under the assumption that everyone on the site is a professional, and publicly visible accounts give attackers easy access to lots of information. LinkedIn appears to be frequently used to gather information to drive phishing campaigns, such as email addresses and job information. This can be used to create spear-phishing campaigns that target specific industries or positions within a company, with a higher success rate. Data can be gathered either by adding people with a fake account or by scraping millions of publicly visible accounts.

Fake Profiles / Spear Phishing – A 2020 phishing attack on LinkedIn, involved fake profiles that would contact victims, primarily targeting business owners and key decision-makers. The attacks used a fake OneDrive login page to steal Microsoft credentials. These fake profiles were hard to spot at a glance, since they would generally have large networks of connections that were relevant to the victims, making them appear legitimate.

How can you protect your business?

Whilst there are any number of spam-filtering tools and technologies in the market, the best way to prevent attacks is to educate your people about the potential threats, as they are your first line of defence.

We've helped companies develop holistic cyber strategies to improve their security online. This includes awareness training for staff and customised phishing attacks to see how susceptible the workforce might be. Needless to say, the results are often surprising to an organisation. However, this information enables training to be provided where it's needed and nurtures a more pragmatic and cost-effective approach to security education.

Nobody should be paranoid about the messages they receive, but they deserve to be safe in a world increasingly reliant on email and instant communication. If phishing is responsible for starting 91% of all cyber-attacks then by knowing how to spot and avoid it, you've just tremendously improved your organisations', and indeed your own, security online.

To find out more about how phishing works and how to protect yourself and your business online, take a look at our cyber security course on our online academy.

How we can help!

Our dedicated cyber resilience team can work with you to design, implement and optimise pragmatic controls to ensure your critical data and systems are always protected – helping you sleep easier at night. We recognise that no 'one size fits all' when it comes to cyber security, so our services are tailored to suit your needs. If you are looking for help, then please get in touch!