Social Engineering and Cyber Security

With the mass adaptation of social media and increased information sharing, many of us are more susceptible to forms of so-called social engineering. The proliferation of social engineering techniques from scammers resulted in a rise of cyber-attacks and information compromises throughout recent months. Before discussing the specific types of attacks resulting from social engineering, let's begin with a simple definition.

What is Social Engineering?

Simply put, social engineering is the process of influencing individuals or groups of people through manipulation to give up sensitive information unwittingly. It presents a considerable risk in the world of data protection, and over the course of the pandemic, many of us have found ourselves in positions where we might be vulnerable to the effects of social engineering. Last year, Madeline Howard of cyber-security tech firm Cygenta, contributed to our newsletter on the prominence of social engineering risks in cyber-security. Since then, the threat continues to grow.

270% in 2021

It was estimated that cyber-attacks resulting from social engineering techniques increased by 270% in 2021, in the wake of more computing becoming cloud-based. Read on to find out more about this threat landscape.

COVID-19 Phishing Attacks

Phishing attacks aren't new – and they are probably here to stay. Cybercriminals are always looking for new themes to use to engage us, and sadly, they have exploited COVID-19 due to the heightened levels of emotion and uncertainty surrounding it.

667% increase in phishing scams

It has been reported that there was a 667% increase in phishing scams in one month alone during the pandemic. We have seen a considerable rise in COVID19-related phishing attacks that prey on our willingness to help others, our financial worries, concerns about PPE, testing, cures, and discount codes to name a few.

The rise in phishing attacks – and COVID-19-themed attacks in particular – is a reminder that cybercriminals will exploit our emotions, particularly during a crisis. If you receive a communication that you're not expecting, which asks you to do something and makes you feel emotional, be aware, this could be social engineering.

Twitter Hacks

Recent common attacks have also reminded us that phishing is not only carried out over email. In July 2020, we saw the extraordinary compromise of 130 high-profile celebrity Twitter accounts through vishing (voice phishing).

The hackers obtained the phone numbers of a handful of Twitter employees. They used social engineering techniques, such as friendly persuasion, to gain their usernames and passwords, giving them access to internal systems. The criminals subsequently compromised high profile accounts, sent tweets, accessed private direct messages, and downloaded sensitive content. Twitter observed: 'This was a striking reminder of how important each person on our team is in protecting our service.'

continued

This hack was an illustration of the different methods used by cybercriminals to engage us with their scams. It is important to remember that all organisations, even the most tech-savvy, can fall victim to social engineering – and that raising awareness of cyber security is crucial for all businesses across all industries.

Ransomware in Hospitals

UK stats published by the National Crime Agency found that in the first 3 months of 2021, the number of reported Ransomware attacks was already three-times higher than those reported for the full year of 2019. Ransomware is an unforgiving attack at the best of times, let alone when it impacts healthcare during a global pandemic. Ransomware spreads through a network and locks down data with a promise that it will be unlocked when the ransom is paid. In September last year, hospitals in the US and Germany were targeted with ransomware attacks.

It was reported that a woman died in Germany after the ambulance services were incorrectly informed that an A&E department was closed when transporting a person in urgent need of medical attention. This resulted in a diversion to a hospital that was further away, delaying the patient's treatment, tragically resulting in her death. This miscommunication was the result of a ransomware attack. Unfortunately, those who are well-versed in technology are still vulnerable to social engineering. This event became the first death directly linked to a cyberattack on a hospital.

In the US, hospitals in California, Florida, North Dakota and Arizona were forced to use pens and paper due to their digital systems being locked down.

In May of 2021, the US oil and gas supplier Colonial Pipeline was the victim of a huge ransomware attack that left the business unable to operate because the hackers left them unable to access key data. They ended up paying the hackers ransom of £3.7m to regain access to their systems. The whole attack was reportedly due to a single leaked password.

Closer to home, the National Cyber Security Centre reported that it was involved in a record number of cyber incidents involving ransomware over the last year, with a large number of nefarious activity originating from Russia. In many cases, hackers were seizing corporate data and asking for cryptocurrency in return.

To protect ourselves from ransomware, we must always be vigilant when clicking links and downloading files spread by social engineering. The spread of ransomware also reminds us of the importance of regularly backing-up data, storing these back-ups offline and testing them to ensure they are working as we would expect.

Lessons to Carry Forward

More of us than ever are now working from home, which has come as a welcome convenience to many. However, we should not forget the lessons learned from some of the biggest cyber security incidents of the last couple of years. We must move into 2022 feeling empowered by technology and confident in using it securely.

Reflecting on lessons learned is one of the most powerful ways we can understand the cyber security threat landscape – and be better prepared for and protected from the attacks of tomorrow, encouraged by social engineering or otherwise. If you want to learn more about how you can protect your clients from the risks presented by the evolving world of social engineering, check out our cyber page.