Presented by HIROC

BRIT

writing the future

why do people fall for phishes?

Ransomware is fast becoming one of the most common types of cyber-attack, with even the most unsuspecting people aware of its existence. As recent high-profile incidences of Netwalker ransomware attacks on institutions have shown, ensuring an organisation is educated and equipped to protect against this growing threat is vital.

With new threats increasing, cyber literacy is vital for the continued success of businesses and organisations. At Brit, our goal is to help you face a more secure future. Along with Dr Jessica Barker of Cygenta, we're here to give insight into navigating this ever-changing cyber landscape.

The evolution of ransomware through phishing

The first known ransomware was created in 1989, and now, over 30 years later, ransomware has evolved to be one of the most prevalent forms of cyber-attack. It has changed from something pretty basic to a much more mature form of attack.

We now see ransomware being used as a distraction tool to mask more complicated forms of cyber-attack. We've also witnessed the emergence of 'leakware' or 'extortionware', in which your data is not simply locked up; it's also stolen. The cybercriminals threaten to publish the data unless you pay the ransom.

There are many different ways that ransomware can spread, some of which are technical. However, the most common threat vector is phishing. Those scam emails designed to look like they come from your bank, boss or best friend and encourage you to click a link, download an attachment or transfer money. Sometimes they're incredibly easy to spot, but other times they are much more sophisticated.

One of the most common misconceptions of why phishing attacks are so commonly successful is the idea that people are stupid if they fall for a scam. The reality is we're all susceptible to being scammed or tricked by these sophisticated tricks.

continued

So, why do people fall for phishes?

One reason is that many people simply do not understand the harm that can be wrought from clicking a link or downloading an attachment. A linked issue that we face is that many people do not comprehend the scale of cyber-crime. Statistics do not mean much when we are trying to convey an unseen, intangible threat; they are too easy to dismiss.

The good news is that we have all become savvier with phishing emails. We know to look out for grammatical errors and to be sceptical of emails from royalty wanting to share their wealth with us. The bad news is that cybercriminals know we have evolved, so they have evolved, too. Many phishing emails are much more targeted now than they used to be, and they try to manipulate us by influencing how we process the information in the emails.

Criminals have embraced Nudge theory. They understand that if they use specific psychological triggers (time pressure, shame, temptation and curiosity, etc.), we are more likely to process the information quickly and not give ourselves time to question before we click. They make us panic, and when we panic, we have less capacity to consider that everything may not be as it seems, meaning our reaction could have unintended consequences.

Protection from the future threat

The criminals move ahead by looking at our behaviour and evolution; by understanding their methods, we can do the same. If you want to learn more about how you can protect your clients from the ever-evolving risk landscape of phishing, check out the insights on our cyber page.