From Zoom to Netflix, your life could be a hack waiting to happen

From Zoom to Netflix, cyberattacks are getting clever about getting your attention.

Anna Collard

In 2020, the world went digital. The global pandemic pushed companies and individuals, not very gently, into the realms of remote working and online meetings and digital engagements.

On one hand, this shove was inspirational. People stopped sitting in traffic, wore comfortable clothes and discovered previously unplumbed depths of productivity. On the other, the cybercriminals were equally inspired. Attacks became more inventive, subtle and clever in their approaches.

According to Anna Collard, SVP Content Strategy and Evangelist of KnowBe4 Africa, they are insidious and dangerous and it’s becoming essential that people learn how to recognise the threats and protect themselves against them.

“Platforms like Zoom and Netflix have seen huge adoption which has meant a rise in attacks,” she explains. “Criminals use increasingly sophisticated methods to bypass systems that flag phishing attacks and try to trick you into revealing information that gives them access to your accounts, be they business or personal. And as soon as they have this information, they get into your systems and distribute malicious emails to your contacts and dive even deeper into systems and personal details.”

A surge of cyberattacks

Researchers at the firm INKY found that from March to August 2020, there was a rush of attacks trying to steal Office 365 credentials using spoofed login pages. Emails were sent from compromised accounts in legitimate companies and because they are from a trusted source, people fall for them and hand over their credentials. The result is that the next company is compromised, and the next, in a domino effect that ripples across industry and individual.

“They trick people by sending them to a fake Office 365 page to verify their login details and then they use that information to get into these accounts,” says Collard.

> “ *The average phishing campaign lasts for only around 24-hours but it can take security technologies up to nine hours to catch up. This means that they can send millions of emails and catch out hundreds of people in that windowof opportunity.* ”

Often, the cybercriminals will register new domains or squat on legitimate domains that they’ve managed to gain access to. With the Netflix phishing attack, the hackers used a standard and recognisable CAPTCHA system on the page so that users felt secure and that they were entering their information onto a legitimate page. The CAPTCHA system is used by multiple websites to ensure that bots are kept out and provide a sense of security, but the hackers leveraged this to lead people to a fake site that then took their details and used them for nefarious purposes.

“The result? Even those who may be more aware of security risks fell for the CAPTCHA page and the scam,” says Collard. “It was extremely clever and preyed on the fact that people assume that the presence of certain things on a website mean it is secure and legitimate. The problem is that many people still don’t know how to identify a legit domain from a fake one and now this needs to become an essential part of security awareness and training campaigns.”

Cyber crime is evolving

And training is the name of the game when it comes to security. The hackers are constantly evolving and changing their tactics and people are being caught unaware by scams that can damage them both financially and reputationally. The impact is far reaching, into personal and business lives, so the best offence is a great training defence.

“It has become essential that people are educated around the risks, are au fait with the clever tactics being used, know about the latest scams, so they can identify some of the most common threats,” concludes Collard. “This is the only way to minimise the risk of being duped and maximise personal and professional protection.”