Scammers prey on vulnerable with 'You're fired!' email

By Anna Collard

2 Sep 2020

Scammers worldwide have been exploiting people's fears of lost jobs and income during the Covid-19 lockdown, by using phishing mails, fake websites and social media to extract personal information, spread malicious software or defraud unsuspecting victims.

Anna Collard, SVP content strategy and evangelist of KnowBe4 Africa

According to Kaspersky's spam and phishing report for Q2 2020, one technique used by scammers was to pose as HR employees to send emails informing recipients that they had been laid off. The emails contain malicious attachments that purport to be receipts for two months' salary.

“The employee was informed that the company had been forced to discharge them due to the pandemic-induced recession,” the researchers write. “The dismissal ‘followed the book,’ in that the attachment, according to the author of the e-mail, contained a request form for two months' worth of pay. Needless to say, the victim only found malware attached.”

Banking phishing attacks also took advantage of people's economic woes by sending emails purporting to offer various pandemic-related discounts and bonuses, directing them to links that gave attackers access to the victim's computer or personal information.

Scammers have targeted South Africans hoping for financial relief during the lockdown too: local banks warned customers of phishing scams claiming their UIF funds had been approved, and referring them to an attachment, and fake emails from the government claiming recipients had to insert their banking details on a link to access free funding.

The Department of Labour also cautioned the public about a scam on social media promising people a pay out of R30,000, using a spoofed departmental website asking people to check if their names appeared on a list of those entitled to funds. The goal? Stealing people’s personal information such as bank login details or downloading malicious software.

These scams highlight at least two lessons: First, fear and anxiety are powerful inducements to getting people to open malicious email. Second, consider the role organisational policy can play here. Do people expect to receive such important notices by email? They probably shouldn’t.

Exploiting pandemic disruption

The disruptions wrought by lockdowns around the world presented a wealth of opportunities for scammers who took advantage of newly remote work environments and supply chain interruptions to target victims.

Kaspersky researchers report that they observed a spike in voice phishing scams at the end of the quarter. These scammers sent emails posing as Microsoft directing recipients to call the Microsoft Support Team at the phone number supplied in the email.

“The share of voice phishing in email traffic rose noticeably at the end of Q2 2020,” they write. “One mailshot warned of a suspicious attempt at logging in to the target’s Microsoft account, originating in another country, and recommended that the target contact support by phone at the supplied number. This spared the scammers the need to create a large number of fake pages, as they tried to get all the information they needed over the phone.”

Scammers also took advantage of global shipping complications by sending fake notices of delivery delays. Other scams mailed targets claiming their packages could not be dispatched due to restrictions on certain types of goods, directing them to an attached archive which opened remote access to the victim’s computer.

New-school security awareness training can enable your employees to make smarter security decisions by teaching them how to recognise these tactics.

ABOUT THE AUTHOR

Anna Collard, SVP content strategy and evangelist of KnowBe4 Africa