Dream job or worst nightmare? New scam targets victims on LinkedIn

LinkedIn users are being warned of new wave of phishing scams that promise a dream job, and target people in the Middle East, Turkiye, Africa (META) region. Cybercriminals posing as HR managers from high-end fashion brands are luring victims to download fraudulent files with the intent to steal credentials for Facebook Business accounts and run ads for monetary gain. Kaspersky experts say cybercriminals are focusing on users from the UAE, Turkiye and Nigeria specifically.

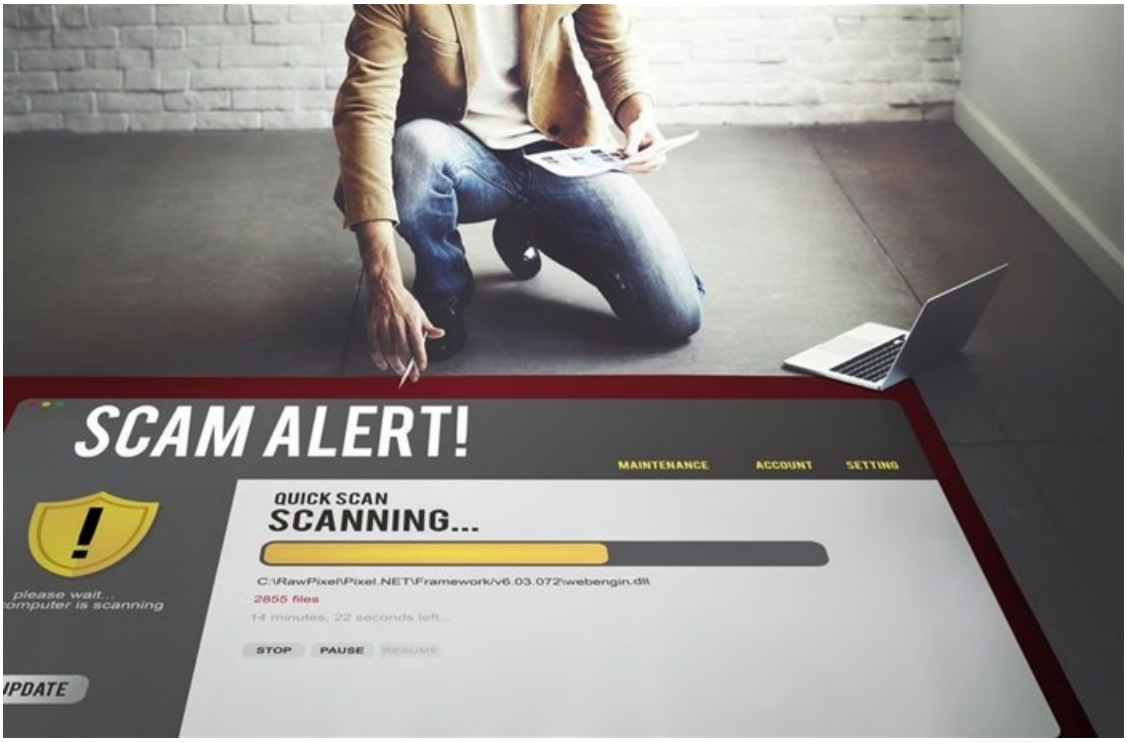

Image source: raw pixel – 123RF.com

People working in the field of digital marketing and sales are prime targets for this scam. As a first step, the scammers proactively contact victims on LinkedIn highlighting a lucrative salary package for a job role. After gauging the victim's interest, the scammers share a malicious link and persuade candidates to download documents related to the job from a cloud storage platform to successfully meet their objective.

Upon investigating the malicious files, Kaspersky experts found that scammers were using a malware named Ducktail to infiltrate devices. Ducktail is designed to steal user logins and passwords for Facebook Business accounts and uses stealthy techniques to remain undetected. The scam is targeted at the META region, with detections in the UAE, Turkey, Iraq, Nigeria and Lebanon.

Sharing her experience to warn people of this ongoing scam, Hiba Safadi, marketing manager from the UAE said: "When the recruiter contacted me, I was intrigued. To know if he was genuine, I checked his LinkedIn profile which seemed authentic because it had a picture, testimonies etc. As we continued our conversation, he repeatedly insisted that I download some files related to the job, and this is when I felt something was off. Since I did not comply, he deliberately started mentioning the salary package to convince me into downloading the files, and this was the second red flag."

Amin Hasbini, Head of Global Research and Analysis Team (GReAT), for META at Kaspersky, said; “This is not the first time Ducktail malware has made a comeback. Enticing people with a dream job that includes a hefty remuneration is a classic example of a social engineering tactic commonly used by scammers. Scammers are capable of communicating from accounts that look like corporate addresses, but in reality are compromised or from free email services or phishing domains. We understand it is very difficult to constantly be on alert, but it is necessary to remain cautious and take basic measures into consideration. For example, understand how the recruiter found you, research the employer, make sure you have a security solution installed, and most importantly, avoid clicking on links or downloading attachments from unknown or suspicious senders.”

To protect employees and organisations with social media business accounts from falling victim to this scam, Kaspersky recommends:

- Restrict access and establish rules for the use of social media business accounts.
- Create a strong password and refrain from using the same password for other websites.
- Companies should use two factor authentication to safeguard online business accounts.
- Companies should ensure BYOD devices are also protected.
- Ensure you have a security solution on your personal devices.
- Do not access business accounts through a personal device.
- Avoid accessing business accounts via public Wi-Fi.

For more, visit: https://www.bizcommunity.com