Top phishing scams to look out for in 2023

Your company's information is valuable, and unfortunately, cyber criminals are relentless in their pursuit of getting their hands on your data so they turn around and sell it for profit. Cyberattacks increase 50% year-over-year, with a company falling victim every 39 seconds. According to the Ponemon Institute and IBM, the average total cost of a data breach was $4.24 million in 2021.

Cyber scams continue to evolve as well and to protect yourself and your company, you should be aware of how to identify these scams in the first place.

Here's a list of the top phishing scams that you might encounter in 2023.

1) Voice Phishing- Typical spam calls are easy to detect as you won't recognize the caller. However, voice phishing is more elaborate, as cybercriminals will masquerade as trusted family members, friends or even company officials. The call will seem personal as they want to gain your trust. Be wary of any scammer pushing you to give out valuable information, and never visit a site they provide over the phone.

In addition to voice phishing, cybercriminals have also gone mobile and will sometimes target victims through text, known as smishing. Read those texts thoroughly and if something feels suspicious, it's best to delete the message.

2) Social Media Phishing- Posting personal information online across social media platforms is very common. Still, when it comes to your company's information, you'll want to be much more careful about what's published and accessible.

   A new scam called spear phishing, is a targeted attack by cybercriminalswho have gathered information from publicly available sites like social media. Often impersonating executives from within the company, employees fall victim to well-crafted and personalized emails that can contain malware to download. Always be alert to any unusual requests and aware of suspicious activity on social media profiles asking you to click on links or open pictures.

3) Business Email Phishing- Probably the most common phishing trend that will continue into 2023 is compromised emails, as more than 90% of cyberattacks infiltrate an organization through email. These typically target businesses or individuals in charge of the company finances as cybercriminals try to gain access to an executive's account to send requests to junior employees. Once an employee does as the email asks, funds are wired to criminal accounts and businesses are defrauded.

Luckily because of the frequency of these attacks, spotting malicious emails is getting easier. Scan the email's greeting, the from email address and the body of the email for noticeable grammar mistakes and spelling errors. Always double-check the hyperlinks included in the email before clicking anything including PDF attachments. When in doubt, it's best to report these emails to IT and security.

Phishing scams are a reality in our digital world and do not appear to be going away anytime soon. Arming your company with proper IT processes and security protocols will help keep your organization safe. Prioritize security awareness training from professionals to arm your company with the skills needed to stop scams in their tracks. Cybercriminals don't sleep so 24x7 threat monitoring like the kind provided by Quercus IT will no doubt go a long way in keeping your company and its data secure.