Don't Get Hooked by Spear Phishing

Recognize These 5 Common Schemes

What hackers want from you: Money and valuable data. Payment authority, employee information, trade secrets, login credentials and other organizational or personal intelligence.

What they use to get it: Information about you. Anything found on social media or your company website or gleaned from deceiving another person that makes their requests look real.

What you should do: Don't engage until you verify. Contact through a trusted channel (like calling on a verified number) before you provide any response or data!

01

CEO Fraud

That odd message from your boss asking for a wire transfer or financial spreadsheet? It isn't really from your boss. Hackers impersonate associates, especially authority figures, to request money or information, often creating a sense of urgency to promote a quick reaction without time to reflect.

02

Lateral Phishing

Don't fall for that link or call requesting your password! Sometimes getting your email credentials is the first phase of a more complex scheme–once acquired, your very real account is then used to phish within the organization. Any unexpected, unsolicited request requiring you to provide your credentials could be the start of a lateral phish.

03

Brand Impersonation

Think that email is from your favorite merchant or vendor? Maybe not. In the past, incorrect logos, unprofessional text, misspellings and poor grammar were indicators of a phish. But phishers have stepped up their game. Microsoft, Facebook and financial institutions are the most often impersonated.

04

Search Engine Phishing

Did you see that Bank XYZ has a credit card with 0% interest for 10 years! And JobSearch.com offers a salary guarantee? Fake websites are showing up in search results, luring with exaggerated prizes and job offers. Don't enter personal information in unfamiliar websites. They may be stealing credentials.

05

Social Media Phishing

Have you ever read or answered a sharing survey on Facebook? Or replied to a personal question on Instagram? Posts and comments like these are turning social media platforms into ideal phishing venues. And publicly shared personal details put the person at risk of becoming a target of other schemes.

Brought to you by Global Learning Systems