SCAMS, SCAMS, AND MORE SCAMS

BY JAY BORDEN

Scams, scams, and more scams. Do you know the most popular ones? Do you know how to protect yourself and your company?

Let's start with the scams in no particular order.

Phishing is a popular scam because it is easy for attackers to do and, more importantly, because it is so effective.

What is it? Phishing refers to email messages that appear to come from an authorized party such as an executive in your company, a bank, the IRS, a law firm, etc. All are parties you believe you can trust and who might ask for your private information. What might they ask for? Username and password, social security number, date of birth, bank account number, or answers to typical security questions used to reclaim an account after losing the password.

All are very effective in stealing an account. The phishing email may contain a link that goes to a fraudulent site that looks real but steals the information and probably puts malware on your device.

Social media scams are effective because people tend to trust social media posts or at least be less wary. It may be a message or link from someone you know. Or it may be a quiz such as what type of animal are you? Looks like fun. But the questions are designed to gather private information often of the type that are answers to the questions used to reclaim your account after losing the password. There will be a link to the quiz page. Once there you will probably get malware downloaded onto your device.

Job offers are popular when jobs are scarce or working conditions make people look for other jobs. Maybe there are rumors of downsizing, or the company being sold. Whatever promotes panic.

Copyright 2020-2023 OneBrightlyCyber,Inc.

SCAMS, SCAMS, AND MORE SCAMS

CONTINUED

Maybe you are simply unhappy at your present place. The offer is usually for a popular type of job such as working from home, cybersecurity, customer service, etc. The pay rate is typically higher than realistic to attract people. If interested you click a link and enter the type of information found on a resume; name, address, email, age or date of birth, job experience, schools attended and more. But again, these are private information used to steal an account or an identity.

Catfishing is the use of fake identities to gain power over someone. It may be through threats, bullying, manipulation, or to inflict financial harm. Catfishing can be used to shift people's perception of an issue or a person.

Scareware is well known to almost everyone. A pop-up appears on your device screen warning that a virus or other malware was discovered. It usually gives a link to click to purchase protective software that will remove the malware or will connect you to a tech who can remove it. It may offer a phone number to call to be connected to a technician. Both may ask you to pay for the service which requires providing your credit card number.

You will need to download software to remove the malware. What also happens is malware and backdoors are installed that will remain on the device after the call ends. The goal is to steal your information and identity for financial gain.

Online shopping scams are one more that is effective. Cybercriminals create fake stores with very real looking websites and attractive products at attractive prices. Remember the old adage if it looks too good to be true it probably is. Never click a link to go to a store. Type the url into the address bar yourself. And do not go to sites you haven't heard about or are unfamiliar with. Stick to ones you know.

Knowing the types of scams can be helpful. People still make mistakes. One Brightly Cyber can provide notice of compromised information 12-18 months on average before most other cyber services or tools. That gives you time to take the measures that render the stolen information useless to cybercriminals.

To learn all the ways we can help make your company and family safer, visit onebrightlycyber.com, contact OneBrightlyCyber at info@onebrightlycyber.com, or call (888) 773-1920.

Copyright 2020-2023 OneBrightlyCyber,Inc.