Phishing Lessons – Quick Summary

Phishing scams through any means of communication can be dangerous. Knowing how to spot them is crucial. Here's a simple guide that summarizes what you should know:

How Scammers Reach You:

- **Email**: Both personal and work email accounts.
- **Text message**: These usually come from unknown numbers.
- **Social media**: People on social media appear more real. Scammers exploit this being someone that may seem familiar, a friend-of-a-friend, or even a stranger.
- **Messenger and WhatsApp**: They use data communication apps to appear more legitimate.
- **Phone calls**: They may even call pretending to be a person or organization you know.
- **Letter mail**: It's rarer nowadays, but some scams will come in via mail.

What Scammers Want (99% of the time, it comes down to money):

- **Money Transfer**: They want to trick you into sending them money, typically through a source you can't dispute like a prepaid credit card, gift card, PayPal, VenMo, or wire transfer. If they can't get it through you, they may try to get access to your financial accounts directly to steal money.
- **Contacts to Exploit**: Who you know and how they know you can be used by hackers. Hacking an email account, for example, can give them all of your email history and contacts who they can try to exploit by impersonating you or others.
- **Identity Theft**: This is where scammers use your name, birthdate, social security number, and other identifying information to take out loans and credit cards in your name, not paying, and leaving you with the hurt credit and debt.

- **Information Ransom**: Ransomware is where a virus encrypts data on company servers. This can include any number of company files and databases, making them useless. They then ask for money to decrypt the files.
- **Exploitation**: In some cases, scammers can use embarrassing information or photos of you through hacked accounts to try and extort money from you.
- **Intellectual Property**: Scammers will sometimes take internal information about your company and sell it to competitors or others who stand to benefit.

Tricks Scammers Use:

- **Impersonation**: Scammers pretend to be someone you trust, like a bank, friend, boss, or colleague.
- **Urgent Language**: They create urgency or threats to make you act quickly.
- **Appealing to Emotions**: They target people with good hearts and lonely hearts.
- **Suspicious Links**: Be careful with links that look real but lead to fake websites.
- **Attachments**: Avoid opening unknown attachments; they might have harmful documents or software.

How to Spot Scams:

- **Check the Sender**: If the email or text is from an unfamiliar source, be cautious.
- **Check the Message Body**: Look for mistakes in spelling or grammar, as real organizations are professional. If images look low-quality or pixelated, it's usually not real.
- **Hover Over Links**: Before clicking, hover your mouse over links to see the real web address.
- **Verify Requests**: If someone asks for sensitive info or money, contact them through known contact information to confirm.

Stay Safe:

- **Use Security Software**: Keep your antivirus and anti-phishing software updated.
- **Activate 2FA**: Turn on Two-Factor Authentication for extra security on all accounts that allow it.
- **Update Software**: Keep all your software updated for better security.
- **Stay Informed**: Keep up with the latest phishing tricks to stay safe.
- **Educate and Report**: Let your colleagues, family, and friends know about phishing scams.
- **Use Filters**: Have good email filters to stop phishing emails.
- **Monitor Accounts**: Check your accounts for anything suspicious regularly.
- **Safe Communication**: Discuss sensitive stuff in secure ways to avoid scams.

By being careful and following these tips, you can spot and avoid these phishing attempts. Always double-check before trusting unexpected messages!

Article website link: *https://www.clarityreached.com/phishing-lessons-quick-summary/*