What is social media phishing?

Social media phishing is when cyber attackers use social networking sites such as Facebook, Twitter, LinkedIn and Instagram instead of email to obtain your personal identifiable information (PII) by baiting you to click on malicious links. It is important now, more than ever, to have an awareness and trained eye to spot and avoid even the most cunning and believable phishing attacks on social media. For example:

You click on a malicious link in a tweet, post, direct message, etc. on your social media that:

- Advertises a gift or some special offer that is hard to resist.
- Warns you to take action to avoid some sort of financial loss. It could look like it’s from a trusted contact if their social media account has been compromised or identity spoofed.
- Takes you to a website which requests confidential information or can infect your computer/mobile device with malware.
- Instructs you to make a phone call to a specific phone number. This can either result in PII requested from you or it goes to a premium rate number that results in exorbitant charges added to your phone bill.

Like fraudulent emails, texts, phone calls, social media phishing plays on human emotions and wants/needs. They can state or imply the urgent need to take action to either avoid an issue or to take full advantage of the bogus offer.

For example, a compromised friend/family’s Twitter account might send you a direct message with a fake link to connect with them on LinkedIn. This link could direct you to a phishing site in order to trick you into giving up your LinkedIn login credentials.

**How do you avoid becoming a victim of social media phishing?**

Just as with any phishing attack, do not be lured by the shiny object.

- **LOOK/THINK BEFORE YOU CLICK.** Do not click on a link in posts/tweets/direct messages unless you are 100% certain they are genuine and safe.
- Make sure the sender’s email address looks legitimate.
- Hover over links to make sure you know their true destination.
- Reputable organizations won’t ask for your credentials in post/tweets/direct messages on social media.
- Don’t be distracted by sensational phrases or offers.
- Think about if it is really genuine would they contact you in this way with this information.
- If you are in doubt, call the correct number of the business or individual from whom the post or tweet claims to be from. Do not call the number that is in post. Verify that number from somewhere else.