Cyber Security: Social Engineering

Mid-America Technology Alliance
Wednesday June 18th, 2015

What is Social Engineering?

Social engineering, in the context of information security, is the art of manipulating people so they give up confidential information.

Social Engineering: Pretexting

Use information from prior research to establish legitimacy in the mind of the victim.

“This is Joel from IT, calling to install the new backup software on your computer.”

“This is John with Customer XYZ, calling to reset my email password.”

Social Engineering: Phishing

Email appears to come from your bank or credit card company requesting “verification” of information with link to fake website.

“Your account has been compromised. Login to your account and change your password.”

Avoid links and phone numbers in emails.

Social Engineering: Phone Phishing

Recreate a legitimate-sounding copy of a phone system on a different phone number.

“Thank you for calling Bank of America. Please enter your 16 digit credit card number now.”

“We were unable to verify your account. Transferring you to a customer care specialist.”

Social Engineering: Baiting

Attacker leaves malware-infected flash drive in a location sure to be found and waits for a victim to use the device.

Label drive as “Work”, “Personal”, “Home”, etc.

Never use unknown discs or flash drives!

Social Engineering: Quid Pro Quo

Something for something. Call victim claiming to be returning call from tech support. Help "solve" problem, and in process, have user type commands that give access or launch malware.

Always verify incoming callers or call them back at known phone number!

Social Engineering: Tailgating

Attacker seeking entry to a restricted area secured by unattended electronic access control simply walks in behind a person who has legitimate access.

Avoid being “too nice”. Holding doors for unknown people carrying large boxes, not questioning people who are on the phone, etc.

Social Engineering: Countermeasures

- Think twice before providing sensitive info or access to unknown people.
- Verify incoming callers or call them back at a known phone number.
- Verify incoming emails or reply to a known email address.
- Avoid using unknown discs or flash drives.

Social Engineering: Contact Info

Jason Klein, CEO
Datility Networks, Inc.
316-282-0774 x3400
jason.klein@datility.net