Texas Council
Risk Management Fund

Phishing Attacks on the Rise

Phishing is the most common type of social engineering attempt. It is the practice of pressuring, tempting, or manipulating people into sending information or assets to the wrong people. Social engineering attacks rely on human error and pressure/scare tactics for success. Phishing attacks come in the form of fraudulent emails, text messages, phone calls, or web sites designed to trick users into downloading malware, sharing sensitive information, or personal data (e.g., Social Security and credit card numbers, bank account numbers, login credentials), or taking other actions that expose themselves or their organizations to cybercrime. The main attack vector for phishing is email, however, new attacks are being carried out via text and phone, as scammers spoof phone numbers so that they appear legitimate. Attacks are also being reported via social media and QR codes. We will look at these techniques and provide some guidance on how to protect your environment and your data.

SMS Phishing

Phishing using mobile or smartphone text messages is called SMS Phishing or Smishing. Most smishing attacks are related to smartphone apps or account management. Recipients may receive a text message offering a prize for paying a bill or stating that your account will be suspended or deleted and prompt you to click on a fraudulent link to "verify your account." Customers who receive these messages are then lured to provide account information such as payment information or account login credentials.

Social Media

Social media phishing employs various capabilities of a social media platform to phish for members' sensitive information. Scammers use the platforms' messaging capabilities—i.e, Facebook Messenger, LinkedIn messaging or InMail, Twitter DMs—similar in ways they use regular email and text messaging. They also send users phishing emails that appear to come from the social networking site, asking recipients to update login credentials or payment information.

Voice phishing

Voice phishing, or vishing, is phishing via phone call. Voice phishing has been around since the days of rotary telephones. Bank scams using telephones was not unheard of even in the 1970's. Voice over IP (VoIP) technology allows scammers to make millions of automated calls per day. They use caller ID spoofing to make their calls appear as if they're made from actual organizations or local phone numbers. Vishing calls typically scare recipients with warnings of credit card processing issues, overdue payments and unpaid debts, or trouble with the IRS. Callers that respond end up providing sensitive data to people working for the criminals. Some individuals end up granting remote access of their computers to the scammers on the other end of the phone call.

QR Code Fraud
QR code fraud, also known as quishing, works much like any other form of phishing, with criminal scammers posing as a legitimate source and attempting to trick people into handing over sensitive information or downloading malware. Quishing uses QR codes that direct victims to their fraudulent website. The technology has become more common in the past few years and users will often find QR codes as the default option for a variety of activities such as links to advertisements, parcel delivery tracking, parking lots, and anything else that might require an individual to access a specific webpage or resource. QR codes obscure the destination of link since the user can simply scan the barcode to reach the source. This creates a prime opportunity for scammers. QR codes force people to interact with the link via their phone, rather than navigating to the resource on a computer or tablet. Phones generally have weaker security protections, which makes it easier for cyber criminals to access with fake links.

Security Awareness is Key
Organizations are encouraged to teach users how to recognize phishing scams, and to develop best-practices for dealing with any suspicious emails and text messages. For example, users can be taught to recognize these and other characteristics of phishing attempts:

- Requests for personal information, or to update profile or payment information.
- Requests to send or move money.
- A file attachment the recipient did not request or expect.
- A sense of urgency ('Your account will be closed today...') or subtle (i.e., a request to pay an invoice immediately) threats of jail time or other unrealistic consequences.
- Threats of jail time or other unrealistic consequences.
- Poor spelling or broken grammar.
- Inconsistent sender address.
- Links shortened using Bit.Ly or some other link-shortening service.
- Images of text used in place of text (in messages, or on web pages linked to in messages).
- Be mindful of QR codes that show signs of tampering.

Organizations can enforce best practices that put less pressure on users to be phishing detectives. For instance, organizations can establish Clarifying Policies – i.e., a supervisor or colleague will never email a request to transfer funds. They require employees to verify any request for personal or sensitive information by contacting the sender or visiting the sender's site directly, using means other than those provided in the message. Organizations should insist that employees report phishing attempts and suspicious emails to the IT Support Team.

The TCRMF Cyber Risk Services Advisor is ready to schedule Cyber Risk Assessments and Incident Response Plan Tabletop Testing visits for members. To get on the schedule, contact Lee Cain, Cyber Risk Services Advisor at Lee.Cain@sedgwick or 512-619-1437.