Cyber Self-Defense: Safeguarding Against Social Engineering Threats

Social engineering is a cunning method fraudsters use to trick people into giving away sensitive information or performing actions that can lead to identity theft, financial loss, or other forms of harm. In today's interconnected world, where we share more personal information than ever before, the threat of social engineering scams looms larger than ever. This week, we'll share some practical tips we hope will help you identify and avoid falling victim to popular social engineering scams.

What is Social Engineering? Before we dive into prevention, it's critical to understand what social engineering is. Social engineering is a manipulative technique used by cybercriminals to exploit human psychology and gain access to confidential information. Scammers often use pieces of real information they've found online to fabricate elaborate and believable stories with the intention of tricking you into providing them with something more. Social engineering can take many forms from phishing emails, text messages, and phone calls, to in-person deception.

Where Do They Get Your Information? To outwit scammers, you need to be aware of where they get their hands on your sensitive information. Here are some of the most common sources:

- **Public Information:** Scammers leverage publicly available information to orchestrate targeted schemes. This could include your full name, address, phone number, and other contact information as well as possible family members or associates.
- **Data Breaches:** Scammers often exploit data breaches where your information may have been compromised. This could include login credentials, email addresses, and even more personal or financial data.
- **Social Media:** Your social media profiles are a goldmine of personal information. Scammers may use what you share to craft convincing, targeted, phishing messages or even to impersonate YOU as they approach your friends and family.
- **Dumpster Diving:** Believe it or not, some scammers still resort to old-school tactics like rummaging through trash for discarded bills, bank statements, or personal letters.

How Do You Stay Safe? Now that you know where scammers commonly obtain your information, here are some tips to help you stay safe:

- **Strong, Unique Passwords:** Create complex, unique passwords for your accounts. Use a password manager to generate and store them securely.
- **Enable Multi-Factor Authentication (MFA):** MFA adds an extra layer of security, making it more difficult for scammers to access your accounts even if they have your password.
- **Privacy Settings:** Review and adjust the privacy settings on your social media profiles to limit the amount of personal information visible to the public.
- **Shred Sensitive Documents:** Invest in a shredder to destroy physical documents containing sensitive information before disposing of them.
- **Monitor Your Accounts:** Regularly check your financial statements for any unauthorized transactions or suspicious activity.
- **Educate Yourself and Your Family:** Knowledge is power. Educate yourself and your loved ones about popular social engineering tactics and how to recognize and respond to them.