05/19/2023: Tech Support Scams

In today's digital age, tech support scams have become a growing concern. Scammers pose as technical support representatives, targeting unsuspecting individuals to gain access to their personal or financial information and computer systems. It's very important to protect yourself from these scams, as they often lead to device compromise, identity theft, and monetary loss. Tech support scams are a real threat, but by remaining vigilant and staying educated, you can protect yourself from falling victim to these deceptive tactics. Here are some key points and best practices that will help you stay safe:

1. **Recognize the signs:**
    - Unsolicited calls: Be cautious of unexpected phone calls claiming to be from reputable tech companies, like Microsoft. Legitimate companies rarely contact customers directly.
    - Pop-up messages: Beware of alarming pop-up messages on your computer or web browser claiming that your system is compromised. These often include bogus contact details to trick you into calling the scammers.
    - Urgency and fear tactics: Scammers may create a sense of urgency, emphasizing the severity of the issue and pressuring you to act immediately. They intend to catch you off guard and to prevent you from verifying their claims.
2. **Avoid providing remote access:**
    - Do not grant remote access to your computer or device unless you initiated the request and are dealing with a trusted professional that you know. Scammers will use this access to install malware, steal your personal or financial information, or even to hold your system hostage for a ransom.
3. **Verify the representative's authenticity:**
    - Ask for identification: Legitimate tech support representatives will gladly provide their full name, employee ID, and contact details. Take note of this information for future reference.
    - Call back using only official contact information: If you're unsure about a caller, independently look up the company's' official contact information and use it to call them back. Do not rely on contact details provided by a caller, in correspondence, or phone numbers found with a simple search. Always visit the company's official website to find this information.
4. **Safeguard your personal and financial information:**
    - Never share sensitive information: Legitimate tech support representatives will **NEVER** ask you for credentials or to provide (or access) your financial information, nor will they ask for your social security number over the phone or by email.