
- **Trust NO ONE:** Be Skeptical of Unsolicited Messages: Be **very cautious** of email messages, text messages, or social media and Facebook messages from people you don't know, ***especially*** if they ask you for **money** or **personal information**. Scammers often create a sense of urgency to make you act without thinking. They may even pretend to be your children, grandchildren, or even your nieces and nephews.

- **Create Strong, Unique Passwords:** Use a mix of uppercase and lowercase letters, numbers, and symbols. Avoid using personal information like birthdays or pet names. Use a different password for each important account (email, banking, etc.). Consider using a notebook to help you keep track of them.

- **Avoid Fake "Pop-Ups" & E-Mail Messages:** Don't respond to or click on pop-up windows on your phone or computer, especially if you don't recognize them. If **ANYONE** on the internet claims to have a photo of you in a compromised scenario AKA, through your webcam or found on the internet **THEY ARE LYING**. It is not real.

- **Recognize Phony AKA Phishing Schemes :** Phishing is when scammers try to trick you into giving them your personal information. Be wary of **emails** or **links** that look like they're from a trusted company (like your bank or a government agency think: Social Security) Some of these "attempts" ***may*** contain spelling errors, unusual sender addresses, or requests for your password or account numbers, Social Security numbers ***and much more***.


- **Guard Your Personal Information:** Never share sensitive information like your Social Security number, credit card details, or bank account numbers via email message, text message, or social media/Facebook messages. Legitimate organizations will ***NEVER*** ask for this information in this way.

- **Be Sure To Use Secure Websites for Online Shopping and Banking:** Look for a padlock icon in the address bar and make sure the website address begins with "**https://**" ("**S**" stands for secure). Avoid making purchases or sharing sensitive information on websites and apps that are "**http://**" only.

- **Be Mindful What You Share on Social Media:** Think before you post. If you wouldn't say it to someone in front of you in the check-out line at the store, then it doesn't belong on the internet. **Remember**: Don't share information that could be used to guess your passwords, such as your mother's maiden name or the name of your first pet. Be mindful of posting about your location or travel plans. Thieves can use these details to steal your credit card information, Social Security details, and ***much more***.

- **Set Up Multi-Factor Authentication (MFA) AKA 2 Factor Authentication:** Whenever possible, enable **MFA/2FA** on your online accounts. This requires a second form of verification (like a code sent to your phone) in addition to your password, making it **considerably** harder for a scammers and thieves to access your accounts.


- **Keep Your Software and Devices Updated:** Regularly update your computer's operating system, web browser, and antivirus software. These updates often include security patches that protect you from new threats. This includes your cellular telephone(iPhone, Samsung, Android) and tablets as well.

- **Be Cautious of Public Wi-Fi:** Avoid logging into financial accounts, shopping, or entering **ANY** personal information when using public Wi-Fi networks at places like McDonalds, The Mall, Starbucks or airports. These networks are often not secure and can be vulnerable to hackers and thieves.

- **Avoid RoboCalls / Scammer Calls:** If you don’t recognize the number calling your telephone, don’t answer the call. Scammers and thieves pretend to be relatives, businesses and the government trying very hard to steal your financial data such as your bank account or Social Security information. **When in doubt**: Answer the phone but **do not say anything** and wait for the other party to address themselves.

- **ALWAYS Trust Your Gut:** If something feels suspicious, it probably is. Don't feel pressured to respond or click on a link immediately. Take a moment to think and, if in doubt, delete the message and call the company or person directly using a phone number you know to be correct.


**And most importantly:**

## NEVER be afraid to ask for help!

Your friends, family, children & grandchildren have a wealth of knowledge far surpassing scammers and strangers on the internet. Asking for help with a computer or internet issue doesn't make you seem weak, bothersome or unintelligent.

We **ALL** need help sometimes.

These Computer & Electronic Repair Shops are **honest**, **local** *and* will do you **no harm**.

**Spacebar** – (419) 517-1313 - 5687 Main St, Sylvania

**Computer Discount** - (419) 897-2897 - 701 Conant St, Maumee

**Keith Stone Computers** - (419) 214-0222 - 5220 Lewis Ave, Toledo

*Created by* Anthony David Zbierajewski - FindToledo.com