idresolution
Your Identity at Risk, Our Solutions at Work™

Cybersecurity Month 2022!

Since 2004 the US Government have promoted Cybersecurity month to heighten awareness of the very real dangers to our online and digitally connected lives. Let's look at our personal Cybersecurity and that in our homes.

Cyber Basics... a reminder

- **Think Before You Click: Recognize and Report Phishing: If a link looks a little off, think before you click. It could be an attempt to get sensitive information or install malware.**
- **Update Your Software: Don't delay – if you see a software update notification, act promptly. Better yet, turn on automatic updates.**
- **Use Strong Passwords: Use passwords that are long, unique, and randomly generated. Use password managers to generate and remember different, complex passwords for each of your accounts.**
- **Enable Multi-Factor Authentication: You need more than a password to protect your online accounts, and enabling MFA makes you significantly less likely to get hacked.**

How Do we Get Sucked In?

PHISHING...is one of the most common forms of cyber scams that you are likely to experience. Here are examples of phishing that might be seen in an email to lure you in:

"We suspect an unauthorized transaction on your account. To ensure that your account is not compromised, please click the link below, and confrm your identity."

"During our regular verifcation of accounts, we couldn't verify your information. Please click here to update and verify your information."

"Our records indicate that your account was overcharged. You must call us within 7 days to receive your refund."

Our Digital Home

Every year, more of our home devices, including thermostats, outdoor lighting, door locks, coffee makers, and smoke alarms, are connected to the internet to create a"smart home." These advances in technology, commonly referred to as the internet of things (IoT), are convenient and may improve efficiency and safety, however they also pose a new set of security risks.

WiFi

Secure your Wi-Fi network. Your home's wireless router is the primary entrance for cybercriminals to access all your connected devices. Secure Wi-Fi and digital devices by changing the default password and username. Check your internet provider's or router manufacturer's wireless security options.

Apps

Most connected appliances, toys, and devices are supported by a mobile application. Apps have the ability to gather your personal information while also putting your identity and privacy at risk. Be aware of downloading new, unfamiliar apps or giving default permissions. Check your app permissions and use the "rule of least privilege" to delete apps you no longer need or use.

Less Is More

Disable location services that allow anyone to see where you are, and where you are not. Limit what information you share on social media from home—from personal addresses to where you like to grab coffee. Keep Social Security numbers, account numbers, usernames and passwords private, as well as specific information about yourself, such as your full name, address, birthday, and vacation plans.

More Information? Call Us... 877 308 9167 www.idresolution.net

How Can We Protect Ourselves

- **Back Up Your Data Regularly.** If you do have your phone hacked/stolen you'll want to be able to remotely erase it. That means you need to have the content backed up and stored elsewhere
- **Protect Your Personal Information.** If people have key details from your life, your job title, birth date, and full name, which you may have shared online, they can attempt a phishing attack on you.
- **Don't Download Unknown Apps.** Look at reviews and research before installing if you are unsure. If you're not confident in safety of an app, do not install it.
- **Don't Click on Unknown Attachments.** It's the most common way to unknowingly download malware.
- **Always Use a Passcode Lock and Use Complex Passwords.** Do not use easily guessable PINs, like birthdays, graduation dates, or basic defaults like "0000" or "1234."
- **Don't Store Passwords On Your Device.** Remembering unique passwords for every account can be difficult. So use a secure password manager instead.
- **Keep All Apps Up to Date.** Even trusted apps can have programming bugs that hackers exploit. App updates come with bug fixes to protect you from known risks.
- **Always Enable Two-Factor Authentication (2FA).** This is a second verification method that follows an attempt to use your password.
- **Don't Use Public Wi-Fi Without a Virtual Private Network (VPN).** Get a VPN Secure Connection encrypt and anonymize your data so unwanted viewers can't see it.
- **If You Connect It, You Must Protect It.** Whether it is your computer, smartphone, gaming device, or other network devices, the best defense is to stay on top of things by updating to the latest security software, web browser, and operating systems.

More Information? Call Us... 877 308 9167

idresolution
Your Identity at Risk, Our Solutions at Work™

www.idresolution.net