24/7 SECURITY SERVICES
Personal • Integrated • Effective

PERSONAL SAFETY BULLETIN

April 2023

Cyber security must be at the top of your personal safety priority list.

Think Before You Click: This is one of the most critical cyber security tips that you can use. Be cautious of the unknown links you receive through emails, messages, or while visiting web pages that are not secure. Clickjacking is among the most common methods hackers use to access personal data.

Use Strong and Varied Passwords: It may be easy to use and remember the same password across multiple platforms for all your accounts, but it makes your account more insecure. So instead, use specific passwords for all your different accounts. With this practice, even if a company where you have an account is breached or hackers have accessed one of your account's credentials, these credentials would not work on other websites.

Use a Password Manager Tool: It may be difficult to remember many passwords for your various accounts, which is why a password manager comes in helpful. A password manager is a program or software to help you store and manage all your passwords. You can access all these passwords using a single 'master key' password. This will help you keep these credentials secured and prevent you from writing down your passwords, which is one of the most unsafe methods of maintaining your passwords.

Set up Two-factor or Multi-factor Authentication (MFA): Generally, you require only your user ID and password to sign into your account, but the MFA service enables you to add extra security layers to the standard method of using passwords for online verification. With this, you will receive a prompt to add another authentication method along with the password, like a code, fingerprint, OTP on your phone or email, etc.

Keep Your Systems Updated: Keep all your browsers, software, and operating systems up to date. The older your system and its configurations are, the longer the hackers have to find and exploit all the weaknesses. Updating them will prevent attackers from using them for enough time until new updates.

Use Firewalls and Anti-virus Software: Hackers can attack your systems and networks through various methods, such as malware, viruses, phishing attacks, trojans, spyware, etc. However, with the help of anti-virus software and firewalls, your system can defend itself against these attacks.

Learn About Phishing Attacks:
In phishing attacks, hackers assume a different identity to trick you so that you provide them with your credentials, click on a malicious link, or open files or attachments that can attack the system with viruses or other malware. This can lead to a ransom attack. Some of the tips you can use to prevent this from happening and avoid getting caught in a phishing scam include: do not open emails from unknown people or sources, hover over the links before clicking to figure out where they direct, and if the link seems unsafe, do not click it, check for any grammatical errors and the ID of the sender.

Don't Use Public WiFi without a VPN
If you are using public WiFi, make sure you use a Virtual Private Network (VPN). A VPN allows your device to be secured as it encrypts the traffic between the server and your device. This makes it difficult for hackers to access your data. If you do not have a VPN on your device, you should use a mobile network or another safer internet connection.