Westwood®

Keep It **Secure**

Things You Can Do to Protect Yourself and Your Information

Be alert and educated

- Always be conscious and aware of who asks you for your information. Are they from a credible source? It is advised to never give any of your important information to someone you don't know.
- Create complex passwords and change them often.
- A complex password should include eight to 12 characters, an uppercase letter, lowercase letter, numbers and symbols. It is important that passwords for different programs are not the same or reused.
- Stay up to date with technology precautions and alerts. Sign up to receive weekly newsletters about evolving technology and information regarding cybersecurity.
- Educate your family and friends, especially if there is a family account or cloud content. It is important to share the value of your family's information within your household.
- What is your risk tolerance? Research or pilot projects can be exciting but also risk failure.

Be a selective sharer – do not give out your information unless necessary

- Be cautious on social media when sharing locations. For example, “checking-in” to a resort out of the country may invite people to presume that your house is left vacant. Other examples include your personal emails, phone numbers and other close information.
- Practice safe surfing and shopping. It is important when purchasing products online that you are only required to give payment information. Do not make these transactions from unreliable sites because you might fall victim to fraud.
- Cut back on data sharing. When accepting cookies and terms and conditions for various websites, make sure
  to read the fine print. If you do not read the fine print, you may unwittingly agree to allow a website to share your personal information and internet browsing habits with third party databases and companies.
- Be cautious while using public computers or connecting to free Wi-Fi. It is important to find a secure Wi-Fi source even if it is in a public setting like a restaurant or coffee shop.
- Review and secure your social media accounts. Privacy features are necessary to keep your information secure. Establish the boundaries you want on your social media accounts regarding who can view your profile or comment as well as the passwords you keep for these applications

Know the red flags

- Pressure to send money. Whether it is over the phone or online, do not share personal or financial information with someone who is pressuring, threatening or harassing you to do so.

- Threatened with law enforcement action. For years, scammers have posed as members of the IRS, cold-calling individuals, demanding Social Security numbers and other personal information under threat of imminent law enforcement action. It is important to never provide such information over the phone or online unless you know and trust the individual or website. Many companies and governmental agencies are aware of this scam and, as policy, will never contact you over the phone and demand that you provide your personal information.
- Do not share personal information with individuals or organizations making such demands. If payment is legitimately required, you should be allowed to use traditional payment methods.
- Cash a check for a stranger. If you are ever approached near or next to an ATM, and an unknown person asks you to cash a check or make a deposit on their behalf, please alert an official at that financial institution.
- Beware of strange messages and unknown links. Spam e-mails are often sent with enticing subject lines. Be cautious and do not open messages or click on links from senders for whom you are unaware. Doing so can lead to device hacking, which can allow scammers access to your personal information.

Plan your plug in

- It is important to always use your own personal jump drives or other USB plug-ins. Unknown sources could contain malware or other invading tactics.
- Do not plug your device into public charging stations. These can be found in airports, malls, conference centers, parks or other commercial buildings. So-called "juice-jacking" is becoming more popular and occurs when your device is compromised from the malware that can be installed by a hacker within a public USB cord or port. If a USB port is compromised, there is no limit to what information on your device that a hacker can access

Keep your devices secure and locked

- Passwords are necessary on your phone, tablet or computer device and act as a first line of defense against information thieves. Please keep these devices locked and secure in order to protect information that is otherwise easily accessible.

Shred sensitive information on a semi-annual basis, if it unnecessary to keep

- Keep a separate bin and use a cross-cut shredder
- This is important because thieves are known for going through trash looking for billing and account details, receipts, birthdates and address information.

Westwood®

Security on Your Phone and Things You Should Know

Below are common issues and growing concerns with mobile security threats that are relevant in the modern world of technology. We advise that all clients, employees and online visitors educate themselves on the following digital threats:

Data leakage

- Data leakage is unauthorized transmission of data from within an organization to an external destination or recipient.
- Data leakage prevention (DLP) is a strategy that ensures end users do not send confidential or sensitive information outside of the organization's network. Several strategies can be in place involving a combination of user and security policies and tools. Specific software can be installed to detect potential data breaches and can prevent such events by monitoring, detecting and blocking sensitive data.

Unsecured Wi-Fi

- It is important that every Wi-Fi source you are connected to is secure. If you need to connect to an unsecure Wi-Fi source, follow these steps in order to connect an IP address and protect your information:
- *https://appletoolbox.com/iphone-cant-connect-to-unsecured-network-fix/*

Network Spoofing

- IP spoofing is a specific type of cyber-attack in which someone attempts to use a computer, device or network to trick other computer networks by masquerading as a legitimate entity.
- Monitoring networks for atypical activity, deploying packet filtering to detect inconsistencies, authenticating all IP addresses and using a network attack blocker can be put in place by an IT specialist to prevent IP spoofing.

Spyware

- Spyware is similar to a computer virus but instead of messing up your hard drive, it allows strangers to snoop on you and your information. Skilled hackers can install spyware on your phone without you knowing it. Once it is on your phone, it can record anything you do, from sending a text to using your credit card information to purchase products online or on an app.
- Don't click on strange links, lock your phone and be careful with secondhand smartphones.

Broken cryptography

- It is most found in mobile apps that leverage encryption. There are two ways in which broken cryptography can be introduced in mobile apps.
  - The mobile app may use a process behind the encryption/decryption that is fundamentally flawed and can be exploited by the adversary to decrypt sensitive data.
  - The mobile app may implement or leverage an encryption/decryption algorithm that is weak in nature and can be directly decrypted by the adversary.
- Impacts if broken cryptography: privacy violations, information theft, code theft, intellectual property theft, reputational damage.

Improper session handling

- Improper session handling is the issue where session tokens or non-expiring sessions within a mobile application, are broken or not handled in the right way. In order to facilitate successful transactions between a user and a mobile app's backend servers, mobile apps use session tokens to maintain state over stateless protocols like HTTP or SOAP.
- Impact of improper session handling: fraud, information theft or business interruption.
- Ways to prevent: To handle sessions properly, ensure that mobile app code creates, maintains and destroys session tokens properly over the lifecycle of a user's mobile app session.

Phishing

- Phishing is a form of fraud in which an attacker masquerades as a reputable entity or person in email or other communication channels.
- It is popular with cybercriminals.
- It typically relies on social networking techniques applied to email or other electronic communication methods including direct messages sent over social networks, SMS text messages and other instant messaging modes.
- How to recognize a phishing email:
  - The use of subdomains, misspelled URLs (typo squatting) or otherwise suspicious URLs.
  - The recipient uses a Gmail or other public email address rather than a corporate email address.
  - The message is written to invoke fear or a sense of urgency.
  - The message includes a request to verify personal information, such as financial details or a password.
  - The message is poorly written and has spelling and grammatical errors.

How to prevent phishing

- Phishing defense first begins with security awareness training
- Install precautionary firewalls and anti-virus software
- Be sensible when it comes to phishing attacks
- Watch out for shortened links, especially on social media
- Does that email look suspicious? Read it again and report as soon as possible – do not open any unknown links
- Be wary of threats and urgent deadlines
- Browse securely with HTTPs

Multifactor authentication

- Multifactor authentication is a security system that requires more than one method of authentication from independent categories of credentials to verify to user's identity for a login or other transaction. Also called MFA.
- Sometimes referred to as two-factor authentication or 2FA (allows you to present two pieces of evidence or credentials when logging into an account).

- You should use MFA whenever possible, especially when it comes to sensitive data you want to protect (financial accounts, health records, investment information, primary emails).
- Examples
- Swipe your bank card at the ATM and then required to enter your PIN (personal identification number)
- Logged into a website that sent a numeric code to your phone, which you then enter to gain access to your account

Westwood's Role

Westwood holds the privacy and security of our clients, employees and colleagues at the highest value and promotes the importance of technological education.