AN ESSENTIAL CHECKLIST

Guarding Against Identity Theft

Individuals and families today are at a higher risk of being the target of identity theft given their tendency to rely on various third parties to manage their active and complex lifestyles.

At USI Insurance Services, Personal Risk Specialists work with individuals to help them safeguard their personal information and stay vigilant about the major threats posed by identity thieves.

The following is a checklist of practical steps many individuals can employ to protect themselves against specific types of threats.

Social Engineering

Social engineering typically involves the use of trickery and old fashion con to obtain personal information such as birth date, credit card number, address, social security number, mother's maiden name, or banking institution, to aid in an attack against an individual.

Practical Steps to Follow:

- Educate members of your household, including children, nannies, personal fitness attendants and other domestic employees about basic security protocols, such as never speaking to strangers or sharing personally identifiable information
- Encourage all household members to properly discard (diamond shredder) opened mail, receipts and all documents containing sensitive information. All household members should limit what they share on social media, and avoid disclosing their whereabouts when away from home.
- Develop strict payment authorization and wire transfer protocols with vendors, assistants, financial advisors, accountants and wealth managers. Requests that do not follow established protocols should be flagged and further reviewed to avoid impersonation scams.

Phishing

Posing as legitimate websites, emails or callers, cyber criminals frequently use phishing to induce victims to reveal confidential information. Email attachments containing malware or links to a spoofed website are commonly used.

Practical Steps to Follow:

- Be cautious of links you click on when using social media. There are many fake apps and plug-ins designed to coerce people into clicking on malicious links
- Secure your home network and all operating systems, including mobile devices, with anti-virus software and firewalls. Use a professional IT security firm if necessary

- Avoid uploading medical, financial or other sensitive information to cloud-based services
- Encrypt your home Wi-Fi network
- Never use personal data as part of your password and avoid password reset questions that anyone could answer by researching you or your family

Public Networks

Increasingly hackers are gaining access to high net worth individuals' personal information by infiltrating public and open Wi-Fi networks available at hotels, cafes, and airports, among others places.

Practical Steps to Follow:

- Use a mobile or tethering hotspot or Mi-Fi rather than a public Wi-Fi.
- If you must use public Wi-Fi, consider using a Virtual Private Network (VPN) that provides additional security and privacy to public networks
- Avoid accessing sensitive data, such as bank information, or engaging in financial transactions (money transfers) while on public Wi-Fi.

Online Vendors

Daily interaction with online vendors increases the risk of your personal information falling into the hands of hackers.

Practical Steps to Follow:

- Vet the security and data management protocols of the online vendors you interact with. Know what they do with the information you share with them and what steps they take to protect that information
- Make sure login username and password is encrypted during transmission
- Opt for vendors that provide multifactor authentication whenever possible

These are only a few of the many practical steps that can be taken to safeguard your personal information. They are not intended to be an exhaustive list of solutions to prevent every form of attack. However, the cost of implementing these steps far outweigh the financial cost and stress of having your identity stolen. Remember, once your personal information is lost or stolen, your risk of ID theft is forever.

To learn more about these and other solutions to help you guard your personal information against identity theft, contact your local USI Personal Risk Specialist.