CYBERSECURITY BEST PRACTICES

FIVE SIMPLE WAYS TO REDUCE YOUR VULNERABILITY

Cyber crime affects hundreds of millions of individuals globally each year with victims often unaware they have even been affected. The sophistication of methods is ever-increasing and even large corporations and governmental institutions (e.g. Anthem, Equifax, the U.S. Securities & Exchange Commission) have fallen victim to egregious security breaches. In absence of a cybersecurity panacea there are basic measures that can be taken to minimize both your exposure and vulnerability.

Remain Vigilant Against Phishing

Targeted attacks attempting to obtain sensitive personal information often take the form of innocuous emails, sometimes disguised as originating from known and trusted sources. Exercise caution when clicking links or opening attachments, even if the email looks like it's coming from someone you know. Hover over links, to see where they're pointing before you click. Malicious links and attachments can collect your login credentials or install malware or ransomware.

Increase the Complexity of Passwords

Avoid using the same password across multiple platforms as doing so provides a 'master key' to cyber criminals, enabling them to gain access to multiple accounts by hacking only one. When creating unique passwords across accounts, keep in mind that a password that is longer and more complex will offer better protection. A University of Miami Publication on cybersecurity details the specific security enhancement gained through increasing password complexity:

> Suppose a client's password is "Spartacus", in reference to his dog—a hacker can instantly crack this password. If the client adds some numbers to the password, so the password is "Spartacus12," a hacker can crack this password in roughly 14 minutes. If the client adds numbers and a special character, so the password is "@Sparta12cus," a hacker will need approximately 275 days to crack it. Even better, if the password is "Sp@rtacusWENT2T0wn," a hacker will need approximately 377 billion years to crack it[i].

Avoid Public Wi-Fi

According to cybersecurity firm Kaspersky:

> The biggest threat to free Wi-Fi security is the ability for the hacker to position himself between you and the connection point. So instead of talking directly with the hotspot, you're sending your information to the hacker…[who] has access to every piece of information you're sending out on the Internet[ii].

www.pacwealth.com
11512 El Camino Real, Suite 350, San Diego, CA 92130 · 858.509.9797 · Fax 858.509.9984 · E-mail: contactus@pacwealth.com

As an alternative to public Wi-Fi, use the cellular data network or a virtual private network (VPN) app to connect to a Wi-Fi network.

Limit Your Social Media Exposure

Personal data can be used to convincingly impersonate you to gain access to your accounts[iii]. While many people enjoy sharing details of their lives on social media, doing so increases your vulnerability to cyber crime in a multitude of ways. Information you share on social media platforms such as Facebook is stored by these companies for utilization in targeted marketing. Even if your privacy settings are highly restrictive, security breaches of these companies have occurred[iv] and can deliver all the information you have posted on these platforms into the hands of cybercriminals.

Cyber criminals have in many instances victimized social media users by simply using seemingly innocuous information shared publicly on their social media accounts[v]. Posting a photo while on vacation can signal you are away from home, leaving you vulnerable to burglary.

Be Wary of Sacrificing Privacy for Convenience

Technological advancement has delivered increased convenience for consumers at the cost of decreased privacy and security. Amazon's *Alexa* recently recorded a private conversation of a couple in Portland and sent the audio recording to someone in Seattle whose number was stored in the family's contact list[vi]. Everything said to Apple's *Siri* is stored on their servers for two years and is shared by Apple with third-parties who specialize in voice recognition[vii]. Facebook and other apps include in their "Terms of Service" language allowing them to track your location and access your microphone[viii]. As mentioned previously, any data collected from you by another party, stored and shared, is only a security breach away from falling into the wrong hands. The utility provided by tech products and apps must ultimately be weighed against your privacy concerns inherent in their use.

---

[i] Bergner, John F. and Chadiwck, Jeffrey D. *Planning for Privacy in a Public World: The Ethics and Mechanics of Protecting Your Client's Privacy and Personal Security*. University of Miami School of Law, 2017.
[ii] https://usa.kaspersky.com/resource-center/preemptive-safety/public-wifi-risks
[iii] *Be cybersecure: How to protect your financial data from hackers*. Capital Group, 2019.
[iv] https://www.nytimes.com/2018/09/28/technology/facebook-hack-data-breach.html
[v] https://www.ibtimes.com/how-burglars-use-facebook-target-vacationing-homeowners-1341325
[vi] https://www.npr.org/sections/thetwo-way/2018/05/25/614470096/amazon-echo-recorded-and-sent-couples-conversation-all-without-their-knowledge
[vii] https://www.tripwire.com/state-of-security/security-awareness/siri-privacy/
[viii] http://money.com/money/5219041/how-to-turn-off-phone-microphone-facebook-spying/