AIG

AIG PRIVATE CLIENT GROUP

CYBERSECURITY AND PRIVACY SETTINGS

Protection when you're competing on the road: Best practices from the experts

When you're on the road competing, your mind is focused on having a successful ride, not potential cyber threats that put your personal information at risk. Extended stays at competitions often require you or your family members to use mobile devices for online reservations, purchases, or banking. **Are you maximizing protection when it comes to your online activities?**

To help identify areas where you might be at risk, AIG Private Client Group, a division of the member companies of American International Group, Inc. (AIG), is pleased to provide the following checklist from the experts at K2 Intelligence.

Cybersecurity

- ☐ **Remember to use passwords that are complex and at least eight characters long.**
  Examples of complex passwords include passwords that utilize combinations of uppercase, lowercase, numeric, and special characters (e.g. #,! $). Such passwords increase the amount of time an attacker has to spend guessing the password. Do not utilize dictionary words alone or easily guessable or obtainable information such as birth dates, maiden name, or pet names.

- ☐ **Use a different password for each application and/or site access.**
  Attackers commonly are able to compromise several accounts because users tend to use the same password for all their logins. By maintaining different passwords for each application, the attacker will be limited in the number of applications they can breach.

- ☐ **Use multi-factor authentication for all accounts that offer this security measure.**
  By requiring multiple factors (typically a password plus a randomly generated 6-digit code sent via text message) to log in to an account, you increase the security of the account and make it more difficult for attackers to compromise.

- ☐ **Keep your operating systems (iOS, Windows, etc.) up-to-date.**
  Updates have the latest security updates and patches. If you do not keep your systems up-to-date, you are exposing yourself to possible vulnerabilities identified in prior versions.

- ☐ **Never open attachments or click links in emails from senders you do not know.**
  Many attackers will embed malware in attachments, host malware on websites, or try to obtain sensitive information such as login details through user interactions with online forms. Think before you click and consider if the message, its instructions and/or attachments are legitimate.

- ☐ **Never use public Wi-Fi. Consider a Virtual Private Network (VPN) when using a public network.**
  When you connect to public Wi-Fi, you are joining a network of devices and users whose security and intentions are unknown and out of your control. A VPN allows for added security and creates a private network even when you are on public Wi-Fi.

- ☐ **Use full disk encryption for mobile devices (laptops, tablets, and smartphones).**
  Full disk encryption is a technique that encrypts the entire drive, even the operating system. Utilizing full disk encryption helps mitigate the risk of confidential information being accessed by an unauthorized person. It helps to prevent an attacker with physical access to the device from accessing the data on the drive itself.

Privacy settings

- ☐ **Limit what you post on social media. Especially when on the road for an extended period of time.**
  Do not let adversaries know where you are and at the same time, where you are not. It poses a risk to your safety and to the security of your assets. Consider delaying your posts and not providing a live up-to-date status of where you are.

- ☐ **Do not allow applications to use your location.**
  Many applications default to automatically use location tagging which will pin-point where you are with your device's GPS location. Do not let adversaries track you with this data.

- ☐ **Carefully limit which applications can access your contacts, calendar, photos, camera, and microphone.**
  When using an application, review the access it has to your personal data. Consider if this application really needs access and what it may be doing with your information.

- ☐ **Never click on the "Unsubscribe Me" links in spam and promotional emails.**
  Clicking on "Unsubscribe Me" verifies that you are a live person. It is better to label the mail as spam or junk mail. Malware/ransomware may also hide in these links.

To learn more, please contact your independent insurance advisor or Jordan Arnold, Executive Managing Director, Head of Private Client Services, K2 Intelligence: +1 917.243.7343 or jarnold@k2intelligence.com.

AIG

K2 Intelligence
Investigations · Compliance Solutions · Cyber Defense

PCG_843Equine_031518