


CYBER ATTACKS DON'T KNOCK AT THE FRONT DOOR

Can You See Who's Entering Your Personal Cyber Space?



You receive an email message from your attorney asking you to update your family's information they have on file. Simple enough. You recall having to do this for your other advisors at some point. So, you click the link and **unleash a cybercriminal who steals your bank account credentials and syphons off about \$100K from one of your accounts** before you notice.

Unfortunately, this type of scenario is becoming commonplace for individuals – and especially those in high-net worth families.

“Given their assets, high net worth families have exposures at least the size of many small companies.”

Source: [Risk & Insurance](#)

Thanks to the wide array of information available on the internet, cyber criminals can easily troll public information files, real estate transactions, and society page announcements to identify highly valuable targets from whom they can scam money. **These include individuals or families who have:**

- Sold a company for profit
- Bought a multi-million-dollar house or piece of property
- Made a significant monetary gift to an alma mater or charity
- Attended a fund-raising gala, and/or
- Made a sizable campaign contribution to a political candidate

WHAT CAN YOU DO TO LESSEN THE CHANCES OF BECOMING A TARGET OF CYBERCRIME? HERE ARE A FEW MITIGATION STRATEGIES YOU CAN CONSIDER:



ENSURE YOUR ADVISORS HAVE STRICT CYBERSECURITY PROTOCOLS

Make sure your legal, accounting, and wealth management advisors are doing everything they can to keep your private information secure. Ask how they specifically secure your data, what standards they use, how often they update them, and what steps they will take to protect you if a breach ever occurs.



BE AWARE OF THE TYPE OF INFORMATION YOU SHARE ONLINE

You may not be able to control everything that's put out on the web regarding your financial transactions or business dealings because of public information disclosures, but you can certainly curb the types of things you and other family members willingly share on social media. As a family, agree on the type of information or photos you will share that will not compromise your privacy or indicate your lifestyle, assets, or anything else that could make you an attractive target to criminals.



RESTRICT PERMISSION FOR OTHERS TO POST ABOUT YOU

While it can certainly be newsworthy if you attend an important fund-raising gala or make a sizable donation to your alma mater, for example, you may want to consider limiting an organization from publishing personal details or photos that highlight your generosity or identify you as a major benefactor. Update permission statements organizations may have on file for you, and turn "on" privacy settings on your social media accounts to make it harder for someone to get information about you and your family.



LEVERAGE TECHNOLOGY SOLUTIONS

Firewalls, anti-virus software, anti-spyware, and strong passwords can all play an important role in keeping your computers, cell phones, apps, and online accounts safe. But hackers are always looking for ways to get around them. So, make sure you always use the latest versions and operating systems to secure your information and avoid weaknesses.





USE SECURE EMAIL PRACTICES

Make sure your legal, accounting, and wealth management advisors are doing everything they can to keep your private information secure. Ask how they specifically secure your data, what standards they use, how often they update them, and what steps they will take to protect you if a breach ever occurs.



BE AWARE OF THE TYPE OF INFORMATION YOU SHARE ONLINE

Phishing emails that trick you into entering your personal information or passwords are still the key way cyber criminals gain access to your accounts. So only open emails from those you know, beware of embedded links, and delete any emails that seem suspicious, have poor spelling, generic greetings, or need urgent action. It's also a good practice to set stringent security controls for your system, use a strong and unique password, enable multi-factor authentication, and, if possible, use email encryption when sharing sensitive or personal information with your advisors.



GUARD YOUR TRAVEL PLANS

Social media posts about your travels can reveal critical information about where you are, and where you are not. Be mindful of what you and your family post that might unknowingly increase your exposure and make you more vulnerable to a criminal's actions. And if you travel by private plane or boat, be aware that connected devices, such as GPS, transmit your exact location, and let criminals know you're not at home.



CONSIDER CYBER INSURANCE

Typically available as an addition to your homeowners insurance policy, personal cyber insurance can cover a wide array of cybercrimes, ranging from cyber and ransomware attacks to data breaches and online fraud. Since all policies are different, it's important to discuss your specific needs and situation with your insurance broker and understand what's covered, what's not, and available coverage limit options.



Need more information about how to protect your household against cybercrimes?

[Contact Us Today!](#)

This material has been prepared for informational purposes only. BRP Group, Inc. and its affiliates, do not provide tax, legal or accounting advice. Please consult with your own tax, legal or accounting professionals before engaging in any transaction.