Be cybersecure: How to protect your financial data from hackers

Individuals can play an important role in keeping their financial information safe from hackers. Here are some simple things you can do to protect your information.

Most attacks start with phishing emails

Targeted phishing attacks on high net worth individuals and families (so-called "spear phishing" attacks) are the result of extensive research and reconnaissance. The emails will look very plausible and convincing because the potential prize is very large. Malicious links and attachments can collect your login credentials or install malware or ransomware.

- Be very cautious about clicking links or opening attachments, even if the email looks like it's coming from someone you know. If you're not expecting the communication, consider reaching out directly to the sender.
- Hover on links to see where they're pointing to before you click.
- Educate family members about the risks of phishing attacks.

Protect access to your financial accounts

Most attacks on high net worth individuals are after the money, in whatever form it takes – credit, shares, cash, cryptocurrency, etc. Protect the accounts where these assets are stored.

- Use strong passwords (12 characters minimum, 16 or more for financial accounts). Some complexity (a mix of upper/lowercase, some digits, some special characters) is good, but longer is stronger.
- Do not reuse passwords across accounts. A data breach of one service will expose the password you are using across other services.
- Use a password manager to generate and store strong passwords.
- Use two-factor authentication wherever possible. It's better to use an app (like Authy or Google Authenticator), but if there are no other options use your mobile phone number to get the two-factor authentication code.
- Do not accept wire instructions via email. Call the financial institution directly for instructions. Have the financial institution reconfirm the transaction in a second call before the wire is released.
- Limit the access you allow to your accounts by household staff and lower-level family office staff.
- Use a dedicated device or computer that you only use for your financial accounts, not for other web activities like email or web browsing.

Protect access to your email accounts

Your email address is used everywhere as part of your login to various accounts. It is very valuable to attackers. With access to your email account, attackers can spy on you, take control of other accounts or phish your contacts.

- Use a strong, unique password on each of your email accounts.
- Use two-factor authentication.
- Use separate email accounts for different purposes.

Protect your privacy and personal data

Personal data can be used to impersonate you convincingly to financial institutions, family offices, service providers or mobile network providers to gain access to your accounts. Personal data can also be used to impersonate you fraudulently to would-be business partners, as your identity is used to exploit your reputation.

- Minimize social media presence, where it's easy to collect useful personal data.
- Control mobile apps access to location, camera and microphone to reduce opportunities for surveillance on where you are, who you're with and what you say.
- Use privacy controls and ad blockers in your browser.
- Educate family members and staff about the importance of not oversharing online.
- Request a credit freeze (from U.S. credit agencies) to prevent access to your personal and credit-related data. Put a credit freeze on family members. Securely store the PIN you'll need to unlock the credit freeze.
- Cover web-enabled cameras and smart speakers when not in use.

Protect access to your home network

Home networks present attackers another way to access your accounts, conduct corporate espionage, steal intellectual property and monitor your private space.

- Make sure the home routers have very strong, unique passwords — not the default passwords that came with the router.
- Put smart devices (TVs, security cameras, smart doorbells, thermostats, audio systems, etc.) on their own separate network to isolate them from your main home Wi-Fi. These types of devices are often less secure, so isolation from your primary Wi-Fi can protect against malware and eavesdropping.
- Check regularly for vulnerabilities in smart devices, and upgrade or replace when a vulnerability is reported.
- Set up a guest network for staff and visitors.
- Configure home routers to not broadcast the Wi-Fi network name.

Other ways to make it harder for attackers

- Don't use public Wi-Fi (hotels, restaurants/cafes, clubs, etc.). Instead, use the cellular data network or use a virtual private network (VPN) app to connect to a Wi-Fi network. It's very easy to eavesdrop on Wi-Fi data traffic and collect account login credentials, webpage URLs, searches and other personal information.
- Delete apps you don't use. They are only collecting your data.
- Back up important data regularly to recover from ransomware attacks.
- Keep the operating system and apps on all your devices up to date.
- Make sure you have antivirus software installed, enabled and up to date.

CAPITAL GROUP®