CHOATE

10 Personal Cybersecurity Tips – Protecting Yourself

High net worth individuals are particularly at risk for growing cybercrime threats, including from e-mail compromises, confidence schemes, ransomware, and identity theft. According to *FinTech News*, phishing attacks have increased by more than 600% over the past year, with cloud-based attacks rising at a similar rate – but there are some important steps that can reduce the likelihood of falling victim to these types of crimes. And because no cybersecurity measures are foolproof, there are a few best practices to keep in mind when responding to incidents that can't be prevented.

1. Vary your passwords

Don't reuse passwords (this includes not using the same root followed by different numbers, like "password1" and "password2"). If your password is stolen but is unique from all of your other passwords, hackers can't break into other sites or accounts.

2. Use a password manager

Use password manager software to safely store all your passwords in one place instead of writing down or remembering credentials for different logins.

3. Opt for multi-factor authentication

Multi-factor authentication (MFA) adds a critical layer of protection by requiring additional verification of your identify before logging into an account.

4. Confirm wire transfer changes or new payments with a phone call

If you receive directions to change a wire transfer to a new location, confirm the change with a phone call instead of relying on email.

5. Be mindful of what you share on social media

Criminals can learn a lot by what you (and your family) are sharing via social media, such as your current location. They can even make connections to your passwords through your photos and posts.

6. Back up your personal files

To reduce the impact of ransomware, back up key documents and photos to a location that is separate and segmented from your network.

7. Be careful of public Wi-Fi

Avoid connecting to public (not secured) Wi-Fi, such as in an airport or coffee shop. If you are not connecting through a Virtual Private Network (VPN), your communications and information can be intercepted.

8. If you're concerned about being a victim of identity theft, freeze your credit

By freezing your credit, no one can open credit accounts in your name such as a credit card or car loan. For more information, visit: https://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs

9. Be aware of phone call scams

Be suspicious about unexpected phone calls from sources that ask for your personal information or require you to pay them directly. Typically, legitimate communication from a company will come from a verified email asking you to call a specific number.

10. Counsel can be helpful

As you navigate the legal, financial, and technical issues that most cybercrime victims encounter, counsel experienced in responding to these kinds of situations can help you decide how best to respond, interface with experts and law enforcement, and attempt to recover stolen funds.

CHOATE

10 Personal Cybersecurity Tips – Protecting Yourself

For more information about cybersecurity threats and protecting your personal data, please reach out to your Choate team or one of the following attorneys:

Kristin Abati
Practice Group Leader, Wealth Management
617-248-5266
kabati@choate.com

Charles A. Cheever
Co-Managing Partner
617-248-4027
ccheever@choate.com

Adam Bookbinder
Partner, Government Enforcement & Compliance
617-248-4806
abookbinder@choate.com