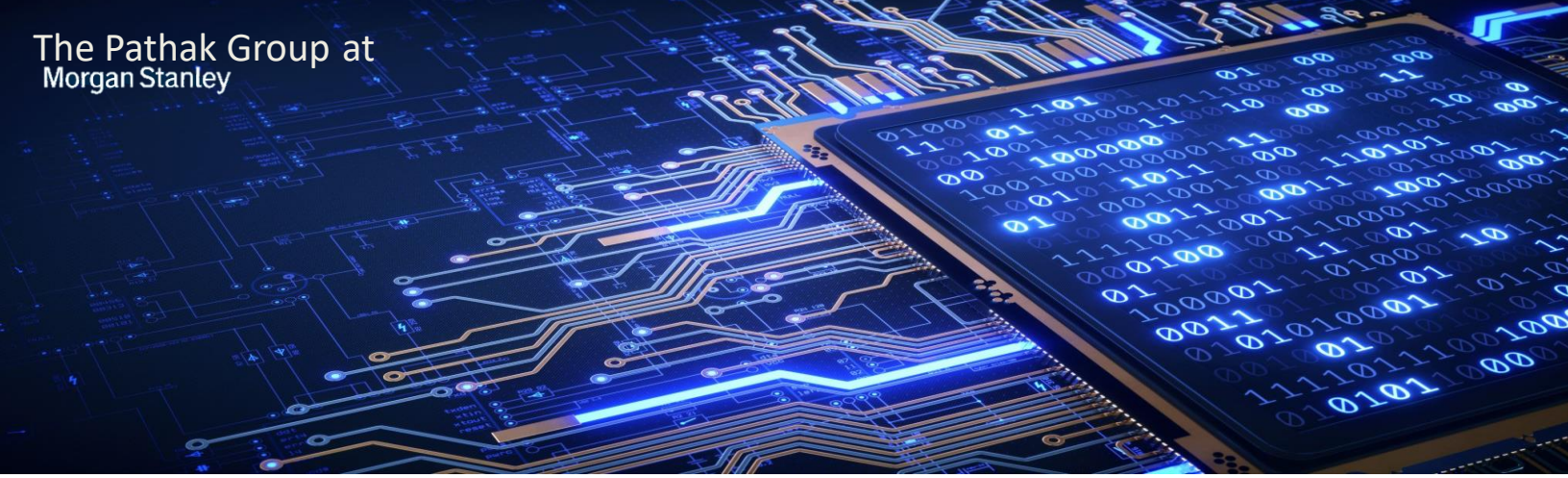

How Should You Respond to Being Hacked?

Stolen Social Security Number

After filing your taxes, you get a notice from the IRS that your submission was rejected because a return under your SSN was already filed. What should you do next?

Report the SSN theft on identitytheft.gov and file a police report. Then, freeze your credit at all major bureaus and make a record of all the fraudulent activity that occurred. Finally, contact us so we can help best protect your assets moving forward.

Hacked Email Account

You start hearing from your contacts saying they're getting emails from your account asking them to wire money to you, or click on a suspicious link. Chances are a cybercriminal stole your email password and now has access to your account. So, what should you do?

Password

Change your passwords to something lengthy and unique. Consider using a password manager to securely store your passwords.

Affected Accounts

Check all accounts that use the hacked email address for unusual activity. Check your social media and your email filters for changes in your accounts.

Going Forward

Use antivirus software on your devices and use multi-factor authentication (MFA) when signing in.

Example of Computer Infected by Malware

Strange ads start popping up on your computer. It's running slower than normal, too. Could be that you fell prey to an online scam and clicked on a phishing link. It's likely malicious software has taken control of your machine. Now what?

Use Antivirus to clean up the malware → Contact an IT professional for additional help → Update you operating system and change passwords

Layer of Protection

One way to protect your accounts from fraud and financial scams is to add a trusted contact. A trusted contact is a person you designate to be contacted if we are unable to reach you or if there are concerns regarding your well-being or suspected financial exploitation.