Punch
A BOUTIQUE INVESTMENT ADVISORY

Wealth Strategies Group

We Are Built for Security

You've been Hacked! How to Combat a Personal Security Breach

Miraya Gran
Client Specialist

I wish I could say in my sixteen years of client service across three different industries that I have not seen a situation where a client was hacked. In our ever-changing, technology driven world, hacking incidents have become far too common. Whether accessing someone's personal email directly, phishing for information via text or social media (smishing), or maximizing scam calls, hackers are becoming increasingly clever with their tactics when attempting to steal an individual's identity. In the United States, it is estimated approximately one in three Americans are hacked every year. The good news is there are steps you can take once you have been hacked to combat the situation.

Beware of Geeks Bearing Gifts

Phishing, one of the most common forms of hacking, is when hackers attempt to trick you into sharing sensitive information. Hackers can even impersonate an individual after they have accessed that person's email. The impersonator then reaches out to the hacked individual's contacts asking for personal information, money, or by offering something compelling, such as a gift card. The author Kevin Mitnick offers this salient warning: "Beware of geeks bearing gifts." Often, these emails contain fraudulent links which allow the hacker to acquire the next individual's email and or computer login. This perpetuates a vicious cycle of access to personal information. Often, the victim is not alerted of the breach until a contact reaches out to confirm whether the emails are legitimate. It is at this point you can take the necessary steps, below, to fight back.

Post Hacking Checklist

Update passwords immediately – Start with updating passwords for your email, your computer, banking and financial institutions, and your social media sites. Make these updates from a different device than the device that was breached. Be sure to use a strong password that is at least 12 characters long, is a combination of letters, numbers, and symbols, and does not consist of any obvious personal information. Each site should have a separate unique password. Don't forget to add two factor authorization on your accounts. A password manager is a great way to keep your passwords organized.

Scan your device for malware – The easiest way to eliminate the source of the hacking is to use a reputed anti-malware and antivirus software to scan and clean your devices.

Reach out to your financial institutions – Making your financial institutions aware of the situation will add a layer of defense with extra eyes watching for impersonated emails and fraudulent attempts to move funds.

Communicate with your community – Informing your friends, family, and colleagues (email contacts and social media connections) of your incident will help prevent them from communicating with or accessing fraudulent links from any impersonated emails that have been sent by the hacker. Communication is key! Don't be reluctant to share about your situation – your communication efforts might help a friend to sidestep a hacking situation. A united front wins the battle!

Pull your credit report – Access your credit report to confirm all activity is legitimate. The four major credit reporting agencies are Equifax, TransUnion, Experian, and Innovis.

Combating Hacking Together

We are happy to be the first call you make upon receiving notice of a personal security breach. Below are steps we can take together to proactively protect you from any further damage once identity theft has been discovered.

Add money movement restrictions – Our Client Specialists can add restrictions to your accounts at the custodian to ensure no money movements occur without the custodian confirming with us first. This will not affect the periodic quarterly withdrawals you have set up but will alert us of any "one-off" money movement requests. A restriction will allow us to confirm the legitimacy of the transaction before it takes place.

Watch for additional suspicious communications – Once we are alerted of a breach by a client, we communicate across the firm to keep an extra eye out for any further suspicious emails or activity.

Open new accounts – Depending on the level of access the hacker has reached, we can work with you to open new accounts and close your previous accounts at the custodian.

Assist in identifying a breach – Do not hesitate to reach out to us and discuss any odd emails, calls, or messages on social media you have received. We will be happy to walk through next steps together. Better safe than sorry is the right motto for these situations! (Trust your gut!) If an email, phone call, or a social media communication feels off, likely it is.

Keeping You Secure

Hacking or no hacking, we take a proactive approach to keeping our clients secure in the following ways.

Helping you get organized – One of the key components in proactively battling identity theft is to be organized with your financial situation. Having a clear understanding of your accounts, their purpose, and their location will allow you to quickly remedy a security breach. Our Wealth Strategies Group is a great resource in getting and staying organized.

Knowing our clients and their communication styles – We take pride in frequently communicating with our clients and building connected relationships with them. This helps us to identify any oddities that occur in a fraudulent email or money movement request.

Using encrypted emails – We encrypt our emails when sending sensitive information such as account numbers, dates of birth, or social security numbers. Be sure to reach out to us and request a secure email when attempting to send sensitive information. The Punch team is eager to keep your information secure.

Training our employees – All employees at Punch receive regular cybersecurity training. This allows us to stay up on the latest trends of hackers and to stay vigilant on your behalf.

Verbally confirming money movement – We confirm any large money movement requests by reaching out to you verbally.

Updating policies – We have cybersecurity, privacy, and disaster recovery policies in place which are regularly updated.

Proper Wi-Fi protections – All working employee laptops have a VPN which secures a Wi-Fi network. Clients and vendors log into a separate Wi-Fi network when in the office.

Experience – Our team comes with many years of client service and industry experience. We have seen and tackled hacking scenarios with clients directly, and we take swift action when these circumstances arise.

A United Front

Staying organized around your financial situation, communicating potential breaches with your network, and building a united front will allow you to remedy a breach swiftly and confidently. We encourage you to make Punch your first call in the event of a personal security breach. Let's be the united front together! ◆