ARTICLES

Cyber Why Do We Need It?

By Sara Neidlinger

Apr 2, 2018

Today, thanks to mobile broadband, we all have more data at our fingertips than we did even 15 years ago.

While this evolution has great advantages, there are also associated risks. Although commercial and corporate attacks garner the media attention, individuals are still also at risk, especially successful individuals and families.

Here are some of the cyber risks you face:

- Phishing -an attempt to trick victims into revealing confidential information with apparently legitimate communication such as a malware-infused email attachment.
- Home Network attack - as businesses tighten security, hackers are turning their attention to individuals where security falls short. Wifi is particularly vulnerable. For example an attacker can create an account named similarly to yours in an attempt to trick you into connecting to it rather than your secured Wi-Fi
- Public Network Wi-Fi - At Starbucks, hotels, cafes, airports are very unsecure and hackers can easily access your communications this way
- Third Parties - this could mean an assistant, employee, advisor or anyone having access to your information
- Cyberbullying - defamation and aggressive strategies on public portals
- Cyber Extortion - attackers access and lock don your computer or data, demand funds

How Can You Protect Yourself

- Create strong passwords
- Don’t share identifiable information
- Use caution downloading information
- Avoid public Wi-Fi networks
- Encrypt your Wi-Fi
- Look for spoofed Wi-Fi networks
- Turn off the UNP feature
- Avoid uploading medical, financial, or sensitive information to iCloud
- Install antivirus & firewalls
- Check your insurance carrier options for protection
- Check with your investment accounts, advisers and brokerages to ensure their funds are protected by

the Federal Deposit Insurance Corp
- Request a security audit of your network and devices

Claims Examples:

Posing as the Boss

When the personal assistant received an email request from her employer asking her to transfer $150,000 into the brokerage account of a familiar sounding third party, she assumed it was a legitimate request and processed it. When she received another email from her employer later that week asking for a second transfer of $90,000, she became suspicious.

Although this email, like the one prior, was sent from her boss's personal email account and included his customary signature and private details of his personal account, something seemed off, prompting the personal assistant to investigate. A phone call revealed that neither request was actually from her employer. Unfortunately, the $150,000 was gone.

Another Unauthorized Transfer

A client of Concentric Advisors noticed a transfer of $25,000 from his account. Upon contacting the bank, he learned that the transfer was made by someone entering his correct username and password in the online banking system. He visited his local bank branch where he changed his login credentials.

Once home, he logged in again from his computer. A short time later, another unauthorized transfer was made. Because his home Wi-Fi and router were not properly secured, the attacker was able to gain access to the connection and log all traffic and credentials being entered.

Does my insurance coverage these scenarios?

Maybe. Cyber loss coverage is carrier-specific and generally very limited or not covered at all. The good news is that insurance carriers are now rolling out specialty lines products specifically for these new risks. Even better, the costs associated with these protection policies are often quite economical.

TAGS:
Private Client