# Cyber Security Event Recap

September 28, 2017

Speaker: John O'Connor

## Understanding Cyber Security

### Who are cybercriminals?

Cybercrime is committed primarily by economic criminals located overseas. These criminals are intelligent, organized, and sophisticated, with certain individuals specializing in various aspects of the attack. Fidelity has not observed a trend in cybercrime being carried out by nation-states (such as China or Russia) or "hacktivists" (those seeking to make a social or political statement.)

### They're always watching

Instead of targeting financial institutions directly, which is difficult because of the firewalls and other protections in place, identity thieves will try to exploit your identity. They pool online data from a variety of sources, such as social networks (Facebook, Instagram, and Twitter), newspaper articles, or data aggregators, to create a targeted and personalized attack. They are looking for exploitable "weaknesses", such as your passions or family members.

### What does a typical attack look like?

In a common scheme called "true name fraud", an online criminal will send you a personalized phishing email. After you click the link or attachment, malware is installed on your machine and lies dormant until you go to a financial institution's website. The software will then activate and record your username and password. Next, online criminals will create an account in your name at another financial institution, under their exclusive control. They will transfer funds from your bank account to this new account and then send the funds abroad, out of the reach of US law enforcement.

### Your computer held captive

Ransomware is a type of attack that often targets small businesses. An online criminal will infect your computer with a virus that locks your machine so that you can no longer open any of your files. The solution is always backing up key information in the "cloud" or on an external hard drive.

### Exploiting the generous

If you have a foundation, beware! Form 990 provides a goldmine to online thieves by showing what charities and causes you support as well as how much you give.

## How can you protect against an online attack?

### Two-factor authentication

Use two-factor authentication on all financial websites. Two-factor authentication requires your username and password plus other information (such as a PIN or code), making it that much harder for hackers to break into your accounts. It's essentially a password that changes each time and that you don't need to remember. However, do NOT use a system that emails you a code, as online fraudsters can break into your email. Instead, the best systems are linked with your phone, either through an app or by texting you a code.

### Consider freezing your credit

This is a powerful tool. Freezing your credit doesn't impact your current credit lines but keeps new creditors from accessing your credit score, making it less likely an identity thief can open a new account in your name.

### Employ prudent cyber hygiene
Only use trusted networks, keep your software updated, and leverage financial alerts.

### Consider malware detection software
Anti-malware software provides the first layer of protection for your computer. Install updates as they become available. Be aware, however, that all malware detection programs are 3-6 months behind cybercriminals. The developers of malware test their code against the latest detection software.

### Isolate your online financial accounts
One additional step is to use a separate device for online financial transactions. NEVER use this device for opening emails or browsing the internet. This way, you have a device "sterile" from any malware. If you do receive an email containing malware, it will have no access to your financial assets.

## Other Security Considerations

### Manage your digital footprint
The more information you have online, the greater a target you are for identity thieves.

Be careful of what you or your kids post online. Don't post vacation plans or any other information that can be used against you.

See what you can learn about yourself online. The more aware you are of your online presence, the more alert you will be to personalized malware attacks.

### Secure your home
Even if you live in a "safe" neighborhood, be on the lookout; you could be targeted based on where you live.

Review your home security system (alarms, cameras, sensors, etc.).

Have an emergency evacuation plan in place and kept up-to-date. What do you need to take in an emergency? Do you know where those items are located?

### Reconsider your household help
One major blind spot in personal security is household help, such as nannies, maids, and gardeners. These people have access to your home and personal information, such as what home security system you have in place or what artwork you have displayed on the wall.

For all household help and those with access to your home, conduct a background check before hiring.

### Travel safely
Traveling to a foreign country puts you at risk to a wide variety of dangers, ranging from injury and illness to terrorist attacks and natural disasters.

Consider these steps when traveling abroad:

- ✓ Register with the state department – make it easy for the local embassy to contact you if needed.
- ✓ Consider purchasing medical insurance that includes evacuation to the US, especially when visiting countries with lower quality healthcare.

### Protect against elder abuse
When it comes to elder abuse, the "bad guys" are often trusted individuals, such as caregivers and extended family members.

Elder abuse has been on the rise in recent years. As a result, we recommend granting at least one trusted individual, whether a friend, family member, or financial advisor, access to view financial accounts and watch for any suspect transactions.

## Q&A Session

### Once I freeze my credit, how difficult is it to "un-freeze"?

It's easier to unfreeze your credit than it is to freeze it. While you freeze your credit with all agencies, you only need to unfreeze with the one that your creditor uses. You can specify the temporary lift for a specific creditor or a certain time period.

### How secure are secondary security questions, such as "What was the make of your first car"?

Unfortunately, these types of questions are not as secure as two-factor authentication. Malware software can still capture this information along with your username and password. Additionally, identity thieves can easily find answers to most questions, such as previous addresses or the name of your school.

### Do passwords auto-saved in Chrome and other browsers protect against malware?

Unfortunately, no. Malware can record all characters that leave your computer, including passwords saved in a browser.

### If I'm concerned that I might have malware on my computer, what steps can I take to protect myself?

- ✓ Purchase anti-malware software and install updates as they become available.
- ✓ Use two-factor authentication on all financial websites. For all clients of Ibis Capital, this is available for your Fidelity.com and Ibis Nest accounts. Contact our office today for assistance with setting this up.
- ✓ If you strongly suspect malware on your computer, consider wiping your computer and reinstalling your operating system. Make sure to save a copy of all personal files before wiping your computer.

### How does Ibis Capital help protect my identity?

- ✓ We verbally confirm all money transfers with clients. Because we have a personal relationship with each client, we act as a guard dog against any suspicious transfers.
- ✓ We do not send personally identifiable information (PII) by regular email. Instead, we use Barracuda email encryption service.
- ✓ We offer two-factor authentication through Fidelity.com and the Ibis Nest to give you an extra level of security in accessing your accounts.
- ✓ We securely store all physical client files and use a secure 3rd party shredding service, Iron Mountain.
- ✓ We have professional end-to-end IT support through Stratos Wealth Partners, our Registered Investment Advisor. Stratos secures all of your data in our workstations, servers, and transmission through various methods, including two-factor authentication, full disk encryption, antivirus software, and VPN. In addition, Stratos offers firewalls and undergoes yearly penetration testing by a 3rd party vendor. To date, Stratos has passed all penetration testing.