# Cyber Security Tips for Finance Professionals

**By: Mike Lazzaro**
**Marketing Content Specialist**
**ABC-Amega Inc**

*As originally published in the Credit Research Foundation 1Q 2019 CRF News*

***Editor's Note: Some of the content for this article was provided by Dave Newell of Loptr LLC.***

Practicing good cybersecurity habits have become second nature in our personal lives. We wouldn't leave our social security number, a credit card or checkbook out when there are contractors at our house, nor would we provide personal information to someone calling to claim they are from our bank or credit card company without verification. These are the same types of things we shouldn't do with our company's information.

Don't leave business data unprotected – it seems simple enough, but companies are under constant attack. It's important to educate yourself as well as your staff to prevent the 'bad guys' from harming your company or your customers. Here are five tips for stronger network security.

## Phish Yourself

Organizations should perform test phishing to prepare for potential legitimate phishing attacks by teaching staff what phishing looks like, making it easier for employees to recognize and prevent these type of attacks from happening. As a best practice, companies should send phishing tests to staff on a weekly basis, as well as educate them on how to prevent spear phishing attacks. A spear phishing attack is when someone from outside of the organization targets a specific individual with the intent to steal data, install malware, or defraud the company financially. An example of spear phishing is when an imposter claims to be someone from inside the company, but who may be out of the office – and asks an employee to wire them money or pay an urgent invoice. In this scenario, the imposter's email appears to be from your boss, a coworker or someone else who has payment authorization abilities (achieved with email spoofing). The underlying theme with phishing and spear phishing is that email can be tough to trust nowadays. If an email seems suspicious, it very well may be. When someone sends you a link or an attachment via email that you're not expecting, be very cautious. When in doubt, send the message to your IT team to review and verify before clicking any links or downloading any files. It is also a good idea to implement a more secure way of trading sensitive files, internally, that doesn't involve email.

## Train Your Team

Understand threats and focus on key behaviors that staff should follow. Focus on critical activities that are in policies, such as Acceptable Use Policy. This policy informs users what the company's rules and regulations are, as it relates to online security. Create posters and reminders to help your team keep security at the top of mind. Companies can also perform live training exercises that simulate cyber-attacks. Cymulate and Skybox Security are companies that can produce a simulated attack. These companies can determine possible threats and weaknesses and prepare a plan to heighten network security. Companies should also continuously train staff on cybersecurity and stress the importance of maintaining safety, both at home and in the office. Employees receive countless fraudulent emails per week, so it is recommended that IT departments communicate any potential threats that might be circulating; and employees should immediately report any suspicious activity they encounter to their IT team.

## Use Better Passwords

There are plenty of ways for hackers to crack passwords by using standard techniques, and this makes both personal and business accounts vulnerable. It is suggested that you don't use your name or children's names for passwords, as well as any common personal information. The National Institute of Standards and Technology (NIST) has suggested that long passwords are better than the previous recommendation for eight character passwords. A good guideline for creating a longer, complex password is to combine three words, capitalize one of them and add a two- or three-digit number. This will create a password that is about sixteen to twenty-five characters in length, which are next to impossible

for people to crack. NIST suggested that these passwords won't have to be changed, unless of course you know for a fact that they have somehow been compromised.

**Use Two Factor Authentication**

Two-factor Authentication is an extra layer of security used to make sure that people trying to access an online account are who they say they are. First, a user will enter their username and password, but before access to the account is granted, they are required to provide another piece of verifying information. The second factor could come from a text message, voice message or a push notification to a cell phone. Once the user is authenticated, access to the account will be given.

**Patch Software**

A patch is a change to a computer program or software that is designed to fix, update or improve it. Patches will fix security vulnerabilities and other bugs. Many companies only look at one aspect of patching, which is to patch the Microsoft Windows Operating system. The truth is that other programs, web browsers, and devices all need to be patched. Hackers have been known to attack audiovisual and telephone systems, which can give them access to much more than just information on a network server. Patching isn't a one and done activity; it should be done as often as patches are sent in, sometimes monthly. If programs or devices give the opportunity, it is a good idea to set up automatic patches, and you'll know that patching is being done as often as it needs to be.

As cyber-attacks become more common, businesses in every industry are falling victim. Companies should continuously educate their employees on security. Being aware of breaches at other companies is not sufficient; neither is a reaction to individual security problems at your own organization. Active involvement is key to addressing the risks of illegal cyber activities.