Financial Services Employers Face Significant Increase In Cybersecurity Threats

Insights
12.10.20

Employers in the financial services sector are facing an unprecedented number of cybersecurity attacks during the pandemic crisis. To put this in perspective, the Financial Industry Regulatory Authority (FINRA) has issued nine notices regarding the ongoing and widespread cybersecurity threats facing the industry since the COVID-19 pandemic began – and only issued seven cybersecurity notices in the 14 years before the pandemic. What do financial services employers need to know about this development, and what can you do to minimize your chances of falling victim to such an attack?

Why Are Cybercriminals Targeting The Financial Services Industry During The Pandemic?
The financial services industry is not alone when it comes to the increased threat of cyberattacks. Cybercriminals have also been targeting many other industries during the pandemic, including healthcare and manufacturing. Criminals have used phishing emails to prey on remote employees, including those who have inadequate cybersecurity at home, those who may not be complying with company electronic policies at home, and those who are simply too distracted at home to recognize a phishing email.

What separates the financial services industry, however, is how lucrative a successful attack can be. Cybercriminals likely view industry companies as deep-pocket organizations that would be willing to pay significant sums in exchange for the return of confiscated information and for the restoration of their networks in response to a ransomware attack. Malicious actors likely understand that a financial services company can experience significant financial losses if its network is even temporarily disabled, especially in times of great market volatility. Cybercriminals may also be able to profit by misusing the stolen company or customer information.

While cybercriminals have many weapons in their arsenals, they may perceive a higher likelihood of success by specifically using phishing emails for their financial services attacks. In a 2020 report, the cybersecurity company ProofPoint provided its findings after conducting simulated phishing attacks on individuals who worked in 19 different industries across the globe. Overall, individuals in the financial services industry had the highest failure rate in the study. In assessing the most problematic phishing emails, ProofPoint found that individuals in the financial services industry had the second highest failure rate for phishing tests using malicious links, and the third highest failure rate for phishing tests using malicious attachments.

These attacks can be devastating to financial services companies. For example, in December 2019, cybercriminals successfully infiltrated the network for Travelex, a British foreign currency company, in a ransomware attack. The attack reportedly crippled the currency exchange's systems for weeks. Travelex ultimately paid the attackers $2.3 million in exchange for the restoration of its network and the return of its confiscated information. The overall damage to Travelex was estimated to be approximately $30 million and the attack was reportedly one of the key reasons why the company subsequently declared bankruptcy.

What Are The Specific Phishing Scams At Issue?

Through its recent notices, FINRA has repeatedly warned of cybercriminals using sophisticated phishing emails in an effort to infiltrate company networks and to confiscate company and customer information, including through increasingly common ransomware attacks. These phishing e-mails appear to be routine, work-related messages, but actually contain links and attachments that – if clicked or opened by an unsuspecting employee – could expose the system to cybercriminals.

FINRA has reported that cybercriminals are sending emails from the spoofed domain names of "broker-finra.org," "regulation-finra.org," and "invest-finra.org." FINRA has also warned that cybercriminals created the "finnra.org" (with an additional "n") website and may send phishing emails from this domain.

In May 2020, FINRA warned of cybercriminals sending phishing emails from the spoofed "broker-finra.org" domain. The emails appeared to be sent by actual FINRA officers, including the head of its Office of Financial and Operational Risk Policy and its Senior Vice President of Corporate Communications. The malicious actors titled the emails "Action Required: FINRA Broker Notice for [Firm Name]" and requested the recipient's immediate attention to an attachment. In some situations, the attachment was not included in an effort to gain the recipient's trust so that a follow-up email could be sent with an infected attachment or link. In other situations, recipients received what appeared to be a PDF file that, when clicked, directed the recipient to a website that required the recipient to input his or her Microsoft Office or SharePoint password.

In October 2020, FINRA warned of phishing emails from the spoofed "regulation-finra.org" domain, which appeared to be sent by FINRA's Regulation Department. The emails advised the recipient that the organization was updating its conduct and supervisory rules and required the recipient to complete a survey. Most recently, in November 2020, FINRA warned of additional phishing emails that were sent from the spoofed "invest-finra.org" domain.

In August 2020, FINRA advised that malicious actors created the imposter "finnra.org" website, which was designed to mirror its actual website. FINRA warned that malicious actors could also use the finnra.org domain to send phishing emails.

Malicious actors are likely spoofing the finra.org domain because there is a high probability that a financial industry recipient will comply with an email that they believe to be from the regulatory organization. Under the organization's rules, failure to comply with a request from FINRA could

organization. Under the organization's rules, failure to comply with a request from FINRA could result in the suspension of a financial firm's membership or a registered representative's affiliation with a FINRA member firm. Cybercriminals appear to be using this to their advantage, hoping that the recipient will blindly follow the instructions that appear to be from FINRA.

Considerations For Financial Services Industry Employers

You should consider the following steps to reduce the likelihood of a successful phishing attack:

- Educate employees on the recent phishing scams in the financial services industry, including providing the fraudulent domain names and FINRA guidance issued to date on the known scams currently being perpetrated by cybercriminals within the industry.
- Provide training on how to identify a phishing email and the procedures to follow when an employee receives a suspicious email.
- Perform phishing drills, sending test emails to employees requesting that they click on a link or open an attachment. Based on the number of employees who fail the test, your organization can better determine how susceptible you would be to an actual phishing attack and can make determinations on the need for additional employee training. Additionally, individuals who fail the test may be identified for additional training and education.
- Monitor FINRA notices to stay apprised of new scams that are specifically targeting the financial services industry.

If you have any questions regarding how cybersecurity threats could impact your organization, or best practices for addressing those threats, please consult your Fisher Phillips attorney.

Related People

Jeffrey M. Csercsevits
Partner
610.230.2159
Email

Service Focus

Privacy and Cyber

Industry Focus

Financial Services