
Login
******
Password
****

It's Open Season for CYBER CRIME

By Jeffrey Bernstein
Managing director of cybersecurity
and data privacy advisory services
Marcum Technology LLC

Computer hackers have stepped up their attacks during the COVID-19 crisis

President John F. Kennedy once said that, "In a crisis, be aware of the danger but recognize the opportunity." Soon after the nomination of President Barack Obama, Rahm Emanuel, Obama's soon-to-be chief of staff, echoed those words by telling the *Wall Street Journal*, "You never want a serious crisis to go to waste."

Maybe no one has taken more advantage of the opportunities presented by a crisis than domestic and international computer hackers. Commercial mortgage finance companies need to be extra vigilant in what has become both a time of crisis and an opportunity for cybercriminals. ▶

Layout by Chuck Howard

◀ **Crime** continued from Page 45

As a result of the global COVID-19 pandemic, the commercial and residential mortgage sectors have been left more vulnerable to a cyberattack. Numerous businesses have temporarily closed and are having trouble making their rent payments. Homeowners — many of whom are newly unemployed or underemployed — are unable to make their monthly mortgage payment. Banks and other lenders holding these notes are offering various forms of mortgage deferral or foreclosure relief.

Although this scenario represents a crisis for business owners, homeowners and mortgage lenders alike, it also presents countless opportunities for fraud. Entities such as Fannie Mae, Freddie Mac and Sallie Mae, and regulators such as the Federal Trade Commission have reported a spike in these scams, many of which are aided by companies that fail to properly authenticate and authorize their users.

Gone phishing

Cybercriminals and hackers employ numerous methods to attack financial institutions and extract information. Phishing attacks are methods used by hackers and fraudsters to inject malicious code into a computing network or device with the intent to steal information, disrupt operations, obtain ransom payments or deploy malicious devices known as "botnets." The security systems and procedures of the impacted institutions typically lack depth and sophistication.

These scams are aptly named because they typically use lures to hook the user. For phishing attacks to be successful, the hacker exploits a weakness once the computer user makes a mistake. Individual users need to be "tricked" into clicking on malicious links or attachments, giving up their user password combinations, visiting dubious websites or installing malware.

Fraudsters have widely used the opportunity presented by the COVID-19 crisis to deploy ransomware and other malware to machines owned and operated by commercial mortgage borrowers, lenders and third parties that do business with them. The scam is simple, and either the lender or the borrower is targeted. In the former scenario, a hacker pretends to be a current client or new customer seeking commercial mortgage assistance, remittance or abatement. An email also can sometimes contain malware or a "hook" by which the malware is later installed on the system or network.

The flip side of this is when a borrower receives information from what appears to be a lender offering mortgage or other financial assistance. The email and attached documents seem properly formatted, and include information about the Coronavirus Aid, Relief and Economic Security (CARES) Act or some other abatement program. In so-called "man-in-the middle" schemes, the fraudster may masquerade as the lender during an email exchange to gain sensitive information.

These phishing lures work extremely well because they look legitimate. They can be especially effective during a crisis for a number of reasons. During an economic downturn, for example, the content may be of higher interest to the borrower or lender. If people are waiting to receive information about CARES Act assistance, payroll protection loans or loan forgiveness, for instance, they are more likely to accept and respond to communications that seem to be legitimate. In other words, they need help and let their guard down.

COVID-19 also has tended to put companies in a weaker security position. Employees are more likely to work remotely using personal devices from insecure home networks. In the early stages of the health crisis, it was much more difficult for companies to control information flows. Security controls tended to be lax or even nonexistent.

At the end of the day, the result is the same whether the borrower or the lender's employee is targeted in a phishing scam: One of the parties is duped by the hacker and sensitive information is exposed. A fraudster can sometimes obtain access to credit cards or other financial information; wire-transfer or similar funds-transfer instructions; or intimate personal information, such as social security, banking, payroll and tax information.

Watering holes

The COVID-19 outbreak also has enabled hackers to set new traps. Abatement and forgiveness programs incentivize people to log onto a website and provide information, and this was certainly true of the government programs established under the CARES Act. As a result, tricksters have created new "watering holes," which are fictitious and poisoned websites that look similar to legitimate lenders' sites.

Continued on Page 48 ▶

Jeffrey Bernstein is the managing director of cybersecurity and data privacy advisory services for Marcum Technology LLC. Bernstein advises clients in highly regulated industries on the protection of their networks, applications, systems, data, devices, people and property. Marcum Technology LLC is based in New York and is a member of the Marcum Group, one of the largest independent public-accounting and advisory-services firms in the nation, with offices in major business markets throughout the U.S. and select locations overseas. Reach Bernstein at jeffrey.bernstein@marcumllp.com. Follow him on Twitter @Jeff_Bernstein1.

◀ **Crime** continued from Page 46

With so-called "fat finger" websites, for example, the hacker redirects traffic using a similar web address (such as morgatelender.com instead of mortgagelender.com) to lure the borrower. Then they trick borrowers to pony up security credentials or financial information intended for actual lenders. This trick can be done in conjunction with spam emails that direct borrowers to these websites or even more sophisticated schemes.

If the goal is to harvest credentials, the scammers will then use client authorizations to log into the lender's site. They will not only have access to the borrower's information but may even have the ability to do funds transfers from the site. By the time the transaction gets to the closing stage, the hacker has already redirected and stolen the money. With lenders' resources stretched thin, and with telephone service centers being overloaded, there is a tendency to redirect people to self-service websites. Hackers know this and are taking advantage of it.

Other fraud schemes used by hackers during the pandemic are business email compromise scams. Email accounts have been taken over, spoofed or redirected, as well as other forms of communication, including Zoom, chat, instant messaging and others. Once the email account is compromised, a borrower may be tricked into transferring funds to a fraudster's account. Millions of dollars, potentially, have been stolen and transferred to accounts in Singapore, China and other countries. Numerous lawsuits have been filed related to determining who is legally responsible for these fraudulent transfers.

> "There is some good news. Commercial mortgage companies can take some simple and inexpensive but effective steps to protect themselves."

Protecting your company

There is some good news. Commercial mortgage companies can take some simple and inexpensive but effective steps to protect themselves. To quote another Cold War saying, "Trust but verify."

The most effective way to prevent being phished is to pick up the phone and call a lender, real estate agent, attorney or title company to ask if they sent the email and whether the information is correct. Do not call the number in the email. Use only contact numbers for third parties that you know to be legitimate — the ones stored on your phone, or those listed on their business card or website.

For commercial mortgage lenders and brokers, it's time to heighten your security postures. Hackers know that many lending institutions and small businesses are struggling as a result of the economic downturn. So, use strong authentication with more than one factor. Encrypt all data. Develop your security policies — including those that focus on acceptable usage, data retention and destruction, and secure telecommuting — and make them clear to your employees.

Use antivirus software, and perform vulnerability assessments and penetration testing studies. Importantly, you should have an incident-response plan and a cybersecurity partner that is capable of helping you when you face an incident or a breach occurs. Most important of all is to educate your employees on the importance of remaining vigilant and practicing good digital hygiene. It is critical that training should inject a healthy dose of skepticism into end users, especially when it comes to email and other communication channels. ●