Focus On...

Helping you bring your organization into focus.™

December 2020 • Volume 10, Issue 12

CYBER

Can Credit Unions Keep Up With COVID's Evolving Phishing Threats?

Inside This Issue

From everyone at Focus Audits, we'd like to say thank you for your continued loyalty and faith in us. Put your feet up and have a well-deserved rest this holiday season and let every day of the season be filled with joy.

With more credit union employees working from home than ever before, hackers are on the lookout for security weaknesses on home networks – often through email phishing schemes – that could compromise those institutions' data.

The National Credit Union Administration cautioned the industry early on in the pandemic about ongoing security risks, and the issue has taken on new relevance recently in the wake of more data breaches at retailers and the most recent Cybersecurity Awareness Month.

The annual True Cost of Fraud report from Lexis Nexis also indicates fraud – and its impact on the financial services sector – has increased since the pandemic began. The monthly number of fraud attempts each month for the financial services sector has risen by 14% since last year, but the number of attempts that succeeded is up by 42%, according to the study, released earlier this month. The company's research found that financial firms spend $3.64 for every dollar lost to fraud, a 12% increase from 2019.

The 2020 Phishing Trends Report from Keepnet Labs found that 90% of all successful cyber attacks begin via email. That's backed up by Specops Software, a Sweden-based provider of password management and authentication solutoins that works with many U.S. credit unions, which said more than half of all businesses have seen a rise in cybercrime since working from home became the norm.

Specops cybersecurity expert Darren James said the finance sector, in particular, is reporting an increase in the number of phishing attacks since the pandemic began. Hackers are creating elaborate and convincing emails to fool employees, and concerned staffers sometimes let down their guard and click malicious links or download attachments.

Passwords are often the weak link in cybersecurity because they are used everywhere, James said. Studies have shown that employees of financial companies need to remember an average of 69 passwords, so people often reuse them across multiple platforms.

Credit unions should secure their Windows passwords by preventing employees from choosing weak and leaked passwords. Password-vulnerability scans from vendors can help a credit union understand internal weaknesses surrounding passwords, James said.

They should also enable multi-factor authentication where possi-

Focus Audits Holiday Schedule:

December 24, 2020
Close at 3PM

December 25, 2020
Closed in observance of Christmas

December 31, 2020
Close at 3PM

January 1, 2021
Closed in observance of New Year's Day

FOCUS AUDITS™

CYBER

ble and invest in security training and guidance for staff members on how to securely use their IT systems, James said.

> ***"When we were all in the same office, we could consult a colleague when we received a suspicious email, but working from home prevents people from asking for a second opinion or double-checking a strange request from the CEO," James said.***

Specops reported that 61% of businesses don't require complex enough passwords for employee profiles, and about 44% of businesses admit to not fully understanding specific password protection terms.

Smaller credit unions often have fewer resources to apply to IT security, but larger institutions may also present a bigger target area for hackers, James said. The more users you have, the more potential cracks in the armor and the bigger the reward.

Source: *Ken McCarthy, October 30, 2020, 5:00 a.m. EDT*

'Return to Office' Phishing Emails Aim to Steal Credentials

Researchers: Employees Lured With Messages About Shift to Workplace

Researchers at Abnormal Security have uncovered a credential-stealing phishing campaign that spoofs internal company memos concerning returning to the office.

The ongoing campaign is believed to have targeted about 100,000 inboxes, bypassing Google G Suite email security, the researchers say.

The fraudsters are using email messages and landing pages that attempt to impersonate the company's internal messaging system and HR department. The emails focus on status updates regarding whether employees can plan to return to working in their employer's offices, reflecting the updates companies have been sending out following the outbreak of COVID-19, according to the Abnormal Security report.

The fraudsters also are trying to create a sense of urgency by using growing concerns regarding company safety protocols during the COVID-19 pandemic. "This email sets a short deadline for when employees must acknowledge that they have received this message and complete the form," the researchers note.

Since the outbreak of the COVID-19 pandemic, the number of spear-phishing emails using the pandemic as a lure has skyrocketed, according to Barracuda Networks.

"Goals of the attacks ranged from distributing malware to stealing credentials, and financial gain. One new type of ransomware our systems detected has even taken on the COVID-19 namesake and dubbed itself CoronaVirus," according to the Barracuda report.

The emails, sent to specific employees, contain an HTML attachment that bears the recipient's name, which lures employees into opening it. The email also contains text that makes it seem as if the recipient has received a voicemail, researchers state.

By clicking on the attachment, the user is redirected to a SharePoint document with new instructions on the company's remote working policy. "Underneath the new policy, there is text that states 'Proceed with acknowledgement here.' Clicking on this link redirects the user to the attack landing page, which is a form to enter the employee's email credentials," researchers note.

Once a recipient falls victim to this trap, the login credentials for their email account are harvested.

Source: *Prajeet Nair, November 30, 2020*

Focus On...

COMPLIANCE

'Twas the Monday Before Christmas

'Twas the Monday before Christmas, when all through the bank
Not a teller was stirring, the ledgers were blank;
The stockings were hung by the front desk with care,
In hopes that big bonuses soon would be there;

The Board members were nestled all snug in their beds,
While projections of profits danced in their heads;
The VPs in their scarves, covered in snowflakes,
Had just settled in for a short winter's break.

When out in the parking lot there arose such a clatter,
I sprang from my desk to see what was the matter.
To the window I flew and pulled up the blinds,
Gazing out, I wiped the legalese from my mind.

The moon shining brightly on new-fallen snow,
Gave the brilliance of mid-day to the landscape below,
When, what to my HMDA-blurred eyes should appear,
But a miniature sleigh, and nine tiny reindeer.

And then, in a jiffy, I heard on the roof's shingles,
The tapping of hooves and a sleigh bell's jingles.
As I let down the blinds, and was turning around,
Through the front doors St. Nicholas came with a bound.

A bunch of good loans he held out in his hand,
And a complete risk assessment, the best in the land,
His eyes twinkled brightly, while his little round belly,
Shook when he laughed like a bowl full of jelly.

He went desk-by-desk, even to the President's,
Filling all the stockings; leaving many presents,
Finally waving a hand, and a smile to me,
He walked outside, and I followed him to see;

Branches swayed as the wind gusted quickly,
And the moon glowed so brightly, almost magically.
I knew in that moment that all would be well.
The examiners would surely be under his kind spell.

As he sprang to his sleigh, petting gently his deer,
And away they all flew, full of good cheer.
But I heard him exclaim, before he flew out of sight,
"Happy Compliance to You, and to All a Good Night!"

- Kelly Sullivan

AWARENESS

Securing The Generation Gap

Trying to securely make the most of today's technology can be overwhelming for almost all of us, but it can be especially challenging for family members not as used to or as familiar with technology. Therefore, we wanted to share some key steps to help secure family members who may be struggling with technology and might misunderstand the risks that come with using it.

Focus on The Basics
Frequently, the best way to help secure others is to make security as simple as possible for them. Focus on the fewest steps that will have the biggest impact.

1. Social Engineering: Social engineering attacks are one of the primary ways most of us are targeted. Explain how scammers and con artists have operated for thousands of years, the only difference now is bad guys are using the Internet to fool us. Give examples, such as phishing emails pretending to be your bank or a package shipment or scammers calling pretending to be Tech Support or the government. Make sure family members understand they should never give their password, credit card, personal information or access to their computer to anyone. Remind them the more urgent the message is the more likely it is an attack. Some criminals prey on our loved ones longing for love and will pretend to be their dream prospect. Finally, be sure they know that if they feel uncomfortable or have questions about an email or someone calling them, that they call you first.

2. Home Wi-Fi Network: Take time to make sure their home Wi-Fi network is password protected and has the default admin password changed. You may also want to consider configuring the Wi-Fi network to use a secure form of DNS such as the free https://www.opendns.com. Secure DNS services not only help stop people from visiting infected websites but can give you control over the websites people can or cannot visit, which can be especially valuable if kids are visiting.

3. Updating: Emphasize that keeping systems, software and devices updated and current makes it much harder for criminals to compromise them. The simplest way to ensure this is to enable automatic updating wherever possible. If you have a device or system that is so old that you cannot update it, we recommend you replace it with a new device that does support updating.

4. Passwords: Strong and secure passwords are key to protecting both devices and any online accounts. Walk your family members through how to create long passphrases. Passphrases may be easiest for them to both use and remember. Another idea is to install a password manager and teach them how to use it. It can allow your loved ones to use the Internet in an easy and secure manner, only having to remember a single password to unlock the vault. Depending on the solution, you may be even able to virtually administer it for them. If that does not work, perhaps have them write their passwords in a book and then store it in a convenient and secure place. For any critical online accounts, such as their financial accounts, you may also want to set up two-step verification. Be sure to have a legacy plan for any online accounts the same way you would prepare a will for physical assets.

5. Backups: When all else fails, backups will save the day. Make sure family members have a simple, reliable backups in place. For many, a cloud-based approach is often the simplest.

Source: *Chris Dale, Principal Consultant at River Security, Certified SANS Instructor*

Focus Audits, LLC
11301 N. US Hwy. 301
Ste. 105
Thonotosassa, FL 33592
(813) 638-8565
www.FocusAudits.com