'NETWORKINGS

A PUBLICATION OF LOCKNET MANAGED IT SERVICES

FALL 2021

locknetmanagedit.com
844-365-4968

A Message from Kris Kilgard, Locknet Division President

Autumn is the season that represents change. Change as it relates to the color of the leaves, the beginning of a new school year, the excitement of the upcoming holidays, all followed by spring's arrival and the opportunity for new growth and the amazing beauty it brings!

Like the seasons, change is inevitable in business too. It can encourage resiliency, influence innovation, generate better efficiencies, all of which often lead to greater outcomes. Although change can sometimes create a bit of discomfort, it propels us forward to experience new and exciting things. Jack Welch summed it up best. "When there's change, there's opportunity!"

Let me take a moment to introduce myself and officially say "hello." My name is Kris Kilgard. I'm the new President of Locknet Managed IT. While I am new to this position, I am not new to our business. I have been with the Locknet family since 2008, and I previously held the role of Vice President of Sales. Although I have just been appointed this month, I'm already settled in and I'm excited and ready to take on the many new opportunities we have ahead of us!

There is no doubt, so much to appreciate about autumn. It's by far, my most favorite season of the year. Not only do I love the beautiful changes it offers, and let's not forget football season and everything pumpkin spice, it's also Annual Client Survey season here at Locknet! This is an important survey for our business because it allows us to uncover many opportunities for change through the eyes of our clients so that we can become better at what we do. The feedback we receive each year is paramount to our strategic planning for 2022. If you are a managed service client, you should have received your survey in the mail in early October. Although the deadline to return it has passed, there is still time to get it back to us before our official planning begins!

Although our survey results allow us to provide swift and meaningful improvements each year, I want to do even more! My goal over the course of the next year is to visit with as many of our client partners as I can to learn how we can better serve their individual needs and play a greater role in their success. My travel plans are already in the works, and I can't wait to hit the road soon! Until then, please feel free to reach out to me with any questions or concerns you might have or even if you just want to say "hello!" I look forward to working more closely with you in the years to come!

Password Attack Methods-Special Edition:
Learn more about some of the primary password attack methods, what they are, what they mean and how you can defend yourself and your business. See pages 2, 3, 4 and 6.

WHAT'S **INSIDE**

LOCKNET
AN EOJOHNSON COMPANY

Cybersecurity Month Reminds Us: Security Awareness is Essential

After 18 years, National Cybersecurity Awareness Month (NCSAM) is more important than ever, as is security awareness training for your staff. Cybercriminals are increasingly more sophisticated, attacking and breaching networks that seemed lock tight only a few years, even months ago—and more threats are emerging daily. That's why all of us at Locknet Managed IT are using our voices to raise awareness of the cyber issues businesses face today.

> Hackers know employees are often a business vulnerability, they frequently focus their efforts on trying to trick your staff.

NCSAM is spearheaded by the Cybersecurity and Infrastructure Security Agency (CISA) and the National Cyber Security Alliance (NCSA). This year's theme: "Do Your Part. #BeCyberSmart." An essential component of being cybersmart is staying up to date with the latest threats, security tools and strategies through security awareness training.

How security awareness training helps your business

Hackers always seem to be a step ahead: read the latest cybercrime headlines and you'll see a remarkable number of sophisticated attacks on businesses of all sizes. And while many companies have equally as sophisticated information technology experts on their side, new threats are always emerging. Worse, a single breach can bring company operations to a halt and damage an organization's reputation for the long haul.

Security education and awareness training serves as a critical link in the chain of protection for your company—and client—data. It empowers your employees to protect your network. Because hackers know employees are often a business vulnerability, they frequently focus their efforts on trying to trick your staff. Attempts may include attacks via phone, emails or other outlets and devices. The goal is to capture valuable financial information, personal data, or information to feed into their scams. Sometimes, cybercriminals will play the long game—gathering this information to use in sinister ways down the road.

Our cybersecurity experts are both up to date on the latest threats and vulnerabilities, and adept at sharing this knowledge with your staff, so they can head off an attack before it starts. The result: your network stays safe and protected, even in the face of the digital world's most sophisticated attacks.

Cybersecurity training for your employees

The need for security awareness training doesn't just arise during cybersecurity month; it's a year-round, evergreen need for businesses of all sizes. Businesses that hope to thrive in the future need to address network security concerns today. Ready to get started? Contact us to learn more about how we can help you with your security awareness training needs and for all of your network cybersecurity protection. Simply call us at 844-365-4968.

Password Attack Methods Explained

And What You Should Know to Prevent Them

A password attack is the most common form of compromise used in a data breach and phishing remains at the top of the list of a cybercriminals preferred method. According to Forbes Magazine, 80% of security incidents were the result of calculated phishing attacks just last year. These attacks were performed by cybercriminals who targeted governments, businesses as well as individuals to steal login IDs and passwords, also known as credentials, compromising anything they could gain access to.

As incidents continue to rise, it's in everyone's best interest to be more vigilant to safeguard their credentials. Because cybercriminals often rely on human error, they use various types of simple social engineering methods to successfully gain access to systems and services. Understanding a cybercriminals method of attack and staying informed can be the best preventative measure to keep from becoming an easy target. Let's look to learn more about some of the primary password attack methods, what they are, what they mean and how you can defend yourself and your business.

> Never share sensitive information with others unless you are sure that they are indeed who they claim to be and if they should have access to the information.

Continued on pages 3,4 and 6.

1. Phishing

Phishing is a form of social engineering and a popular, classic method of attack. Hackers masquerade as a legitimate and trustworthy source attempting to trick an individual into voluntarily revealing their personal information. There are several methods of phishing cybercriminals use, here are just a few examples:

- **Traditional phishing:** An email is received from what looks like a reliable source instructing the victim to reset their password. The unsuspecting target is lead to a fake website to enter their login ID and password, thus voluntarily handing over their credentials without giving it any careful consideration.
- **Spear phishing:** An email is received containing an attachment or link from what appears to be a reliable source such as a co-worker, a charity or known business. It typically has a generic subject. For example, Request, Urgent/Important, Invoice Due, Payment Status, Follow-up, etc. The attachment or link is highly malicious and will contain ransomware or other forms of malware or malicious code.
- **Vishing and Smishing:** Vishing is a term used for voice phishing, or voice fraud and is used to target owners of a mobile or land line device. Smishing is a term used for SMS phishing or text fraud. Both Vishing and Smishing are forms of phishing performed by cybercriminals using voice calls or texting to dupe their victim into believing something is in jeopardy such as their account had frozen, a payment is overdue, or fraud has been detected.
- **Whaling/CEO Fraud:** Several members of an organization receive a fake email disguised as coming from a senior leader of the business requesting sensitive information or asking to perform other tasks, such as the purchasing of gift cards.

What you can do to keep from falling prey to phishing attacks:

- **Play hard to get!** Links in email and online posts are often the way cybercriminals compromise your credentials and your computer. If you are unsure who an email is from, do not respond and certainly do not click on any links or attachments.
- **Be extra cautious!** Generic greetings such as "Dear Valued Customer" or "Sir/Madam" and lack of contact information in the signature block are great clues of a phishing attempt as well as poor grammar, misspellings, and inconsistent formatting. A good rule of thumb is to always check the sender's email address. Pay close attention for altered addresses with additional or omitted characters. Cybercriminals often use an email address that closely resembles one from a reputable company.
- **Think before you act!** Be wary of communications that trigger you to act immediately. Many times, phishing emails attempt to create a sense of urgency, causing the fear that an account or information is in jeopardy.
- **Don't get hooked!** If an email looks phishy, call the sender or company directly or check with your IT team. Often an IT department can tell you if the email you received is legitimate.
- **Ongoing cybersecurity education is a must!** Protect yourself and your business by enrolling in Locknet's **Security Education and Awareness Training** program. It's a small yet critical investment to arm yourself and your business with essential security knowledge to avoid phishing and other risky situations.
- **Implement email security tools.** Tools such as Locknet's **Email Security Anti-phishing** and **Account Takeover Protection** can help you stop targeted attacks and account takeovers. Locknet's **Email Security** provides other layers of protection against spam, email-borne viruses, email encryption and more.

2. Man-in-the-middle attack (MitM)

MitM attack is a form of eavesdropping and is more common than you think. A MitM attack occurs when a cybercriminal sits between two machines to eavesdrop or intercept communications. The goal is to steal information such as login credentials, account information for the purposes of identity theft, unapproved fund transfer or illicit password changes. Detecting a MitM attack can be difficult and it's important to take precautionary measures to prevent them before they occur.

What you can do to help prevent Man-in-the-middle attacks:

- **Use strong Encryption on Access Points.** Having a strong encryption mechanism on wireless access points prevents unwanted users from joining your network.
- **Enable encryption on your router.** If your router is left open, sniffer technology can be used to see the information that's being passed through it.
- **Strong router login credentials.** Changing default router credentials can sometimes become overlooked and its essential they are changed. Not just your Wi-Fi password, but your router login. It's easy for a hacker to gain access to your router administration to change a DNS server to their own malicious server, or worse, infect your router with malicious software.
- **Use a secure Virtual Private Network (VPN).** A VPN can be used to create a secure environment for information within a to help prevent MitM attacks. A VPN uses key-based encryption to create a tunnel for secure communication. If an attacker happens to get on a network that is shared, they won't be able to decipher the traffic.
- **Leverage network security experts!** Deficiencies that can cause MitM attacks must always be addressed. The network and security experts at Locknet can help you implement a **VPN** or perform an extensive **network security assessment** to help you address any potential vulnerabilities in your environment.

3. Brute force

A poorly crafted or easily guessed password is an easy win for any cybercriminal! A brute force attack consists of an attacker submitting multiple passwords or paraphrases with the hope of eventually guessing correctly. These attacks can be simple because many users use weak passwords or practice poor password etiquette, such as using the same passwords for multiple sites or applications. If your password is the key that unlocks the entry into a service, then think of brute force as the equivalent to using a battering ram.

What you can do to help prevent brute force attacks:

- **Use strong passwords!** Locknet suggests a password or passphrase, 15–64 characters in length, using a combination of upper- and lower-case letters, numbers, and symbols. We've included Locknet's **Desktop Guide to Strong Passwords** on page 5 to use as a guideline so you can create your strong password. The Desktop Guide can be detached to keep handy for future reference!
- **Require Multi-Factor Authentication (MFA).** MFA is an additional layer of login protection to ensure that the only person who has access to your account is you. Use it for VPN, email, banking, social media, and any other services that requires logging in. Use an authenticator app on your trusted mobile device such as a smartphone or use a secure token, a small physical device that can hook onto your USB port. Locknet offers a state-of-the-art **MFA** solution for businesses who want to provide that additional, vital barrier to provide a second layer of security to their authentication process.

4. Dictionary attack

A dictionary attack is a type of brute force attack. It relies on the habit of picking "basic" words that could be used as passwords. Quite often an attacker employs a program that cycles through common words such as words in a dictionary or previously used passwords often found on lists obtained from past security breaches.

What you can do to help prevent a dictionary attack:

- **Use strong passwords!** Follow Locknet's Desktop Guide to Strong Passwords on page 5 to create strong passwords.
- **Use Multi-Factor Authentication (MFA).**
- **Be mindful of the information you provide on social media.** Because cybercriminals often do their research by snooping through a victim's social media profile and postings, they can guesstimate specific words that could be used for passwords such as children's names, favorite celebrities, hobbies, etc. Undoubtedly, social media can contain a treasure chest of personal information that people unwittingly use for passwords.

5. Credential Stuffing

Credential stuffing is a method used by cybercriminals to gain access to multiple sites or service by using stolen credentials from known breaches. Credential stuffing is so effective because nearly two-thirds of users reuse their passwords on multiple accounts. By using just one set of stolen credentials, Cybercriminals utilize mechanisms like Botnets to execute multi-front attacks across multiple sites compromising everything from social media accounts, bank accounts and more.

TIP

Steer clear of social media quizzes. They can be password theft traps. What was your first car, pet's name or the sport you played in high school are all common security questions banking and other service sites use to retrieve or reset your password.

How to help prevent credential stuffing:

- **Use strong passwords!** Follow Locknet's Desktop Guide to Strong Passwords on page 5 to create a strong password.
- **Never use the same password for different services!**
- **Enable Multi-Factor Authentication (MFA).**
- **Scan the Dark Web for stolen credentials.** Locknet offers an ongoing **Dark Web Scanning and Monitoring** service that can identify, analyze, and proactively monitor for your organization's compromised or stolen employee credentials.

6. Keyloggers

Keyloggers are a type of malicious malware called spyware designed to track and record every keystroke, such as your login ID and passwords, banking information, credit/debit card details and the like and then reports it back to the attacker. Typically, a user will download the software believing it to be legitimate, only for it to install a keylogger without notice. Keylogger spyware not only targets a keyboard, but there are also other forms of this insidious spyware that can watch you on your system's camera or listen in through your microphone.

How to protect yourself from keyloggers:

- **Use a firewall.** The attacker must send data from your computer to the internet. With a firewall between the computer and internet, the traffic passing through will get flagged and terminated. Locknet's **Blockade**™ managed firewall service is an excellent option to help protect you from Keylogger attacks. Blockade is designed with industry leading technology and services to help businesses protect themselves against security threats. Blockade includes monitoring, gateway security, traffic analysis, reporting, support services and day-to-day firewall management and more.

DESKTOP GUIDE TO

Strong Passwords

Hackers are sophisticated. Strong passwords can beat them at their game.

The key to secure passwords:

1 Combine upper and lower case letters, numbers and symbols

2 Change passwords every 90 days or if you suspect you've been compromised

3 Use a 15-64 character password or passphrase

4 Use multi-factor authentication

5 Use a password manager

6 Never share with anyone!

Passwords to Avoid

- ☒ Names
- ☒ Common phrases
- ☒ Phone numbers
- ☒ Password re-use on many sites/apps
- ☒ Birthdays
- ☒ Consecutive numbers

LOCKNET
AN EOJOHNSON COMPANY

Strong passwords are an easy way to protect your data from cybercriminals!

locknetmanagedit.com • eojohnson.com
844-365-4968

LOCKNET
AN EOJOHNSON COMPANY

locknetmanagedit.com
eojohnson.com
844-365-4968

IOWA
129 Plaza Circle
Waterloo, IA 50701

MINNESOTA
2717 Hwy. 14 West, Suite M
Rochester, MN 55901

1800 East Cliff Road, Suite One
Burnsville, MN 55337

WISCONSIN
1505 Prairie Lane
Eau Claire, WI 54703

3310 S. Kinney Coulee Rd.
Onalaska, WI 54650

505 S. 24th Ave., Suite 204
Wausau, WI 54401

8400 Stewart Ave.
Wausau, WI 54401

The Locknet Blog

IT and Cybersecurity Trends & Tips

Follow our blog for weekly top industry articles written by our experts—delivered to your inbox each week.

LocknetManagedIT.com

Password Attack Methods

From page 2.

- **Use Multi-Factor Authentication (MFA).**
- **Install a password manager.** If remembering a staggering number of credentials becomes too difficult to manage, try using a password manager. Locknet offers a simple to use **Secure Password Management** solution. This solution provides an encrypted, centralized, cloud-based vault that stores and manages your passwords for you safely in one place. Your passwords can be easily searched, changed, strengthened, and uniquely configured automatically.
- **Keep your systems up to date!** Keyloggers and other malware look for exploits in outdated software and can take advantage of them. One of the most critical pieces of security is keeping your systems software up to date. This includes operating systems, browsers, and applications. Keeping on top of a patching cadence will address issues hackers can exploit. **NetxusPlus** by Locknet is an automated IT solution that includes patch management to keep your systems secure, patched, and optimized. NetxusPlus can be customized with other added security technologies such as **Dark Web Scanning and Monitoring**, **Managed Detection and Response**, **Remote Monitoring**, **IT Automation**, and **Vulnerability Management**.
- **Install anti-virus, anti-malware software.** Anti-virus, anti-malware software is a must-have in the current IT landscape, regardless of if you are trying to prevent a password attack. It protects you from various forms of viruses and malware by scanning the files and traffic entering a computer to detect and prevent fake software from loading onto your system. **Next-Generation Antivirus** by Locknet is an enterprise grade solution that detects and prevents virus and malware infections. Locknet actively monitors these threats and can provide their assistance to remediate malware, should it slip through the cracks.

TIP

Never give your MFA code to anyone or accept an MFA request you did not initiate. Change your password immediately!

Preventing password attacks

Your ability to avoid a password attack will improve significantly just by simply heightening your password security. In this article we reviewed common attack methods used by cybercriminals, ways to stay vigilant and the best practices available to help safeguard your credentials. Here's a quick summary:

1. Create strong passwords. Use Locknet's Desktop Guide for Strong Passwords as guidance.
2. Implement Multi-Factor Authentication whenever possible.
3. Adopt an ongoing Security Education and Awareness Training program. Learn more on page 2.
4. Consider a Password Manager solution.
5. Keep software up to date.
6. Invest in security tools such as Anti-virus/malware, Dark Web Scanning and Monitoring, Anti-phishing and Account Takeover Protection and a state-of-the-art Firewall solution.

If you're not sure where to begin or you would like to learn more about any or all of the preventative measures described in this article, the experts at Locknet are here to help. Contact your local Locknet Account Executive to get started. 844-365-4968