1991 – 2021
30 YEARS OF EXCELLENCE
Computer Technologies, Inc.

TECHNOLOGY TIMES

"Insider Tips To Make Your Business Run Faster, Easier And More Profitably"

What's Inside

June 2025

Kim Nielsen, CISSP, CCSA
President & Chief Technology Strategist at Computer Technologies Inc.
(248) 362-3800

"As a business owner, you don't have time to waste on technical and operational issues. That's where we *shine*! Call us and put an end to your IT problems finally and forever!"

Why Is Email Such a Common Method of Cyber-Attack?

Did you know?

94% of all malware in 2025 is delivered via email.

Why is that? What makes email such a popular vector for malware distribution?

Let's find out together!

Why Do Cybercriminals Prefer To Use Email?

Email is ubiquitous – almost everyone uses email for personal and professional communication. With billions of email accounts worldwide, attackers have countless opportunities to reach potential victims.

This massive user base provides cybercriminals with an enormous potential target pool. Meanwhile, crafting and sending malicious emails is relatively easy and inexpensive. Cybercriminals can reach a large number of potential victims with minimal effort when they use email.

They often impersonate trusted brands or individuals to make their emails appear legitimate. This increases the likelihood that recipients will open the email and follow the malicious instructions.

This versatility allows attackers to adapt their methods to different targets and objectives, such as…

- Malicious attachments (Word documents, PDFs, executable files)
- Embedded links to infected websites
- Spoofed sender addresses that look legitimate

Continued on pg.2

Continued from pg.1

Weaknesses in Email Systems

These online email systems have inherent vulnerabilities that make unencrypted platforms very dangerous. Modern email-based malware attacks are becoming increasingly sophisticated, and can exploit common technical risk factors, such as…

- Complex email protocols with multiple potential exploit points.
- Challenges in real-time verification of sender authenticity.
- Difficulty in comprehensively scanning all attachments and links.
- Legacy email systems with outdated security measures.
- Traditional security filters that can't handle multi-stage attacks.

While email is an essential communication tool, it's also a significant potential security risk that requires constant vigilance and sophisticated defense strategies!

The Allure of Social Engineering

Many successful attacks exploit human behavior, such as curiosity or urgency. Phishing emails often use social engineering tactics to trick recipients into clicking on malicious links or downloading infected attachments.

Emails are particularly effective for social engineering attacks. Cybercriminals can craft convincing messages that:

- Appear to come from trusted sources like banks, colleagues, or familiar organizations.
- Create a sense of urgency.
- Exploit human psychology by triggering emotions like fear, curiosity, or anxiety.
- Manipulate recipients into taking quick, thoughtless actions like clicking a link or downloading an attachment.

Sending mass email campaigns is incredibly cheap. Cybercriminals can use automated tools to send thousands of emails with minimal investment, making it a cost-effective method for distributing malware.

To best combat email-based attacks, we need equally strong prevention tactics! That means using encrypted communication platforms for sensitive data, implementing multi-factor authentication on all of your accounts, and partaking in your yearly cybersecurity awareness training with vigor.

Understanding these factors can help in developing better defenses against email-based threats. Regular training, robust email security solutions, and a healthy dose of skepticism can go a long way in protecting against these attacks.

Free Executive Guide: What Every Small-Business Owner Must Know About Protecting And Preserving Their Company's Critical Data And Computer Systems

This guide will outline in plain, nontechnical English the common mistakes that many small-business owners make with their computer networks that cost them thousands in lost sales, productivity and computer repair bills and will provide an easy, proven way to reduce or completely eliminate the financial expense and frustration caused by these oversights.

Download your FREE copy today at
https://www.cti-mi.com/protectdata625/
or call our office at (248) 362-3800

Security Corner

Do Security Questions Make Good MFA?

Ten or twenty years ago, it was common for accounts with extremely personal information on them to ask you to create a security question.

Most Common Security Questions These websites often let you choose which questions you want to answer. Which ones are most common to see in these scenarios?

- What is your mother's maiden name?
- What was the name of your first pet?
- In what city were you born?

Unfortunately, while these questions are common, they are not always the most secure. Why? Because many of these answers can be easily guessed or found through social media or public records.

To enhance the security of your accounts, consider choosing or answering security questions that are…

- Memorable: You should be able to recall the answer easily and consistently.
- Unique: The answer should be specific to you and not easily known by others.
- Unpredictable: Avoid answers that can hackers can easily guess or find online.

Consider using less common questions, too. Some security experts even suggest providing false but memorable answers. For example, if the question is "What is your favorite color?", you might answer with a very specific shade. That makes it much harder for hackers to guess.

For more information about spear fishing, call us at 248-362-3800 or visit: https://tinyurl.com/22t4hkrd

What Is Password Spraying?

Password spraying is a complex type of cyberattack that uses weak passwords to get into multiple user accounts. Using the same password or a list of passwords that are often used on multiple accounts is what this method is all about. The goal is to get around common security measures like account lockouts.

Attacks that use a lot of passwords are very successful because they target the weakest link in cybersecurity: people and how they manage their passwords.

What Is Password Spraying and How Does It Work?

A brute-force attack called "password spraying" tries to get into multiple accounts with the same password. Attackers can avoid account shutdown policies with this method.

Attackers often get lists of usernames from public directories or data leaks that have already happened. They then use the same passwords to try to log in to all of these accounts. The process is typically automated so that the attackers can quickly try all possible combinations of username and password.

Password spraying has become popular among hackers, even those working for the government, in recent years. Because it is so easy to do and works so well to get around security measures, it is a major threat to both personal and business data security. As cybersecurity improves, it will become more important to understand and stop password spraying threats.

How Does Password Spraying Differ from Other Cyberattacks?

Password spraying is distinct from other brute-force attacks in its approach and execution. While traditional brute-force attacks focus on trying multiple passwords against a single account, password spraying uses a single password across multiple accounts.

How Can Organizations Detect and Prevent Password Spraying Attacks? Detecting password spraying attacks requires a proactive approach to monitoring and analysis. Organizations must implement robust security measures to identify suspicious activities early on.

- Implementing Strong Password Policies: Organizations should adopt guidelines that ensure passwords are complex, lengthy, and regularly updated.
- Deploying Multi-Factor Authentication. Multi-factor authentication (MFA) significantly reduces the risk of unauthorized access by requiring additional verification steps beyond just a password.
- Conducting Regular Security Audits. Regular audits of authentication logs and security posture assessments can help identify vulnerabilities that could facilitate password spraying attacks.
- Educating Users. Users should be informed about the risks of weak passwords and the importance of MFA.
- Incident Response Planning. This plan should include procedures for alerting users, changing passwords, and conducting thorough security audits.

Taking Action Against Password Spraying

To enhance your organization's cybersecurity and protect against password spraying attacks, contact us today to learn how we can assist you in securing your systems against evolving cyber threats.

Can My Data Be Removed From The Dark Web?

Removing data from the dark web is extremely challenging due to its decentralized nature and the rapid dissemination of information. Once data is posted on the dark web, it is quickly copied and distributed, making it virtually impossible to remove completely.

Proactive Measures for Protection

- Use identity and credit monitoring services to detect any suspicious activity related to your personal information.
- Enable two-factor authentication and use strong, unique passwords.
- Regularly monitor your online presence.
- Use a VPN to mask your IP address and protect your activity from being tracked.

Best Practices For Data Management

1. Transparency and Consent: Websites should clearly communicate how user data is collected and used. Users should have the option to opt-in or opt-out of data collection, and they should be able to access, modify, or delete their personal information.
2. Data Minimization: Collecting only the data that is necessary for the website's functionality.
3. Secure Data Storage: Encrypting data both at rest and in transit ensures that it remains secure even if intercepted. Regular security audits and updates are also Crucial.
4. User Control: Providing users with tools to manage their data preferences fosters trust and accountability. This includes options to download, edit, or delete personal information.

7 Unexpected Ways Hackers Can Access Your Accounts

1. Cookie Hijacking. Cookies can be used to access your accounts without your password.
2. SIM Swapping. Hackers deceive your provider to transfer your number to a new SIM card they control.
3. Deepfake Technology. Hackers pose as a trusted colleague or family member through realistic audio/video.
4. Exploiting Third-Party Apps. Hackers exploit vulnerabilities to gain access to linked accounts.
5. Port-Out Fraud. Like in SIM swaps, your number is transferred to another provider without your consent.
6. Keylogging Malware. Keyloggers are malicious programs that record your keystrokes.
7. AI-Powered Phishing. AI is used to craft highly convincing emails.