GUIDE TO UNDERSTANDING AND PREVENTING THE MOST FREQUENT CYBERSECURITY THREATS

With last year's evolving remote work environment, the FBI reported a 400% increase in cybersecurity complaints. The FBI Internet Crime Report 2020 showed complaints reached a record high of 791,790, with reported losses exceeding $4.1 billion. That equates to a 69% increase in total complaints over 2019. California businesses alone experienced losses of $500M+.

Understanding the most common cybersecurity threats and educating your team on how to prevent them may mean the difference between whether or not your company is still in business down the road. Read on to learn more about the most frequent cybersecurity attacks threatening your company.

THIS GUIDE WILL COVER THE FOLLOWING THREATS:

- **Business Email Compromise (BEC)**
- **Phishing Attacks**
- **Malware**
- **Password Theft**
- **Other Notable Threats:**
  - **Traffic Interception/Man in the Middle Attacks (MitM)**
  - **Cross-Site Scripting Attacks**

BUSINESS EMAIL COMPROMISE

Business Email Compromise (BEC) is what occurs when an attacker hacks into a company email account and impersonates the real owner. The hacker's intent with BEC is to defraud the company, its customers, partners, and/or employees by getting them to send money or sensitive data to the attacker's account. Per the FBI Internet Crime Report 2020, BEC schemes were the most costly of cyber attacks with an adjusted loss of approximately $1.8 billion.

In order to steal this information, hackers begin with extensive research. They will sift through publicly available information about your company such as website content, press releases, and social media posts in order to find names and titles, company hierarchy, even travel plans from email auto-replies. From there, hackers will try to gain access to a specific email account.

SOME OF THE MOST COMMON EXAMPLES OF BEC ATTACKS ARE:

- **Fake Boss Scam -** a fraudulent email that is sent from an executive's account to an employee instructing them to urgently transfer money. New employees are generally the target.
- **Fraudulent Invoice Scam -** a cybercriminal uses an employee's hacked email to send notifications to customers and suppliers asking for payment to the cybercriminal's account.
- **Fake Attorney Scam -** A lawyer's email address is used to contact clients, requesting that they pay more money immediately to keep things confidential.

PREVENTING BEC ATTACKS

Most BEC attacks rely on social engineering techniques making them imperceptible to antivirus, spam filters, or email whitelisting. The most effective way to protect your company from BEC attacks is through employee education.

Training should include:

1. ***Don't open any emails from unknown parties.*** If you do, don't click on links or open attachments. These emails often contain malware that can access your computer system.
2. ***Double-check the sender's email address.*** A spoofed email address frequently has an extension similar to the legitimate email address. For example it may come from markc@fuse-three.com, instead of the legitimate email: markc@fuse_three.com.
3. ***"Forward," instead of "reply" to business emails.*** When you forward an email, the correct address must be manually typed in or selected from the address book. This ensures that you use the intended recipient's correct email address.
4. ***Always verify before sending money or data.*** Make it a standard operating procedure that employees call contact to confirm email requests before sending financial or other sensitive data. Be sure that you use a known phone number and do not rely on the number listed in the email.

Educating employees of possible threats is key to preventing any future successful attacks. Part of the company's SOP should include, "When in doubt, double check everything."

PHISHING ATTACKS

Phishing Attacks are aimed at tricking employees into supplying the scammer with personal information. Typically, their goal is to steal passwords, account numbers, or Social Security numbers. With this information, they can easily gain access to emails, banks, or other accounts.

Thousands of phishing attacks are launched every day, and many are successful. The FBI Internet Crime Report 2020 showed $54 million was lost due to Phishing Attacks alone last year.

Phishing Attacks look like they are from a trusted company or source. Most commonly, the email will look like it is from a bank or credit card company, a social networking site, an online payment website or app, or an online store.

SOME OF THE MOST COMMON EXAMPLES OF PHISHING ATTACKS INCLUDE:

- A notice of suspicious activity or log-in attempts
- Claiming there is a problem with your account or payment information
- Requesting confirmation of personal information
- Submission of a fake invoice
- Requesting the recipient click on a link to make a payment
- A notification stating the recipient is eligible to register for a government refund
- A coupon for free items

PREVENTING PHISHING ATTACKS

Most phishing emails are filtered out by spam. Scammers are aware of this and are always trying to outsmart spam filters. It is a good idea to add in extra layers of protection.

Preventative Measures:

1. ***Use Security Software.*** Be sure to set software to update automatically so it is equipped to combat any newly conceived security threats.
2. ***Use Multi-Factor Authentication.*** Many accounts offer additional security by requiring two or more credentials to log in to your account. Multi-Factor Authentication most frequently comes in the form of a passcode sent via text message or an authentication app but can also take other forms to verify identity.
3. ***Backup Your Data.*** If you aren't operating in the Cloud, make sure to backup all data regularly and store copies of the files to an external hard drive.

Like BEC Attacks, the key to prevention is making team members aware of what a Phishing Attack can look like. When in doubt, double check everything.

MALWARE

Malware has been around since the inception of the internet and continues to be a consistent problem. Shorthand for Malicious Software, Malware is an unwanted piece of programming or software that installs itself on a system. The coding in the software is designed to cause extensive damage to data and systems, or to gain unauthorized access to a network. Malware often spreads itself to other systems in the organization. Most strains are spread via a link or executable file sent through an email. Others are delivered via instant messaging or social media.

TYPES OF MALWARE

Virus

Just like the biological variety, viruses spread quickly. They attach their malicious code to clean code, waiting for an unsuspecting user or automated process to execute them. Once activated, they cause damage to core functionality of systems, corrupting files, and locking users out of their computers.

Worms

Worms weave their way from an infected machine through a network. Spreading the infection from consecutive machines. Worms can infect an entire network of devices very quickly.

Spyware

Spyware is designed to “spy” on the user of the infected computer. It collects information without the user knowing, such as credit card details, passwords, and other sensitive information.

Trojans

Similar to the tactics of the Greek soldiers of yore, Trojan malware hides within or disguises itself as legitimate software. It breaches security by creating backdoors and allowing other malware variants easy access.

Ransomware

Also known as “scareware,” ransomware exacts a heavy price. The attacker encrypts the victim’s files then demands a ransom. Access to the victim’s data will not be restored until the ransom is paid. Instructions are sent for how to make payment in order to receive the encryption key.

PREVENTING MALWARE ATTACKS

There are two angles of prevention to protect against Malware Attacks: protective tools and user vigilance:

1. ***Protective Tools:*** Protective tools are easy to implement. You can and should have best-in-class antivirus software that is set up to manage and update itself.
2. ***User Vigilance:*** Such as with all other types of cyber attacks, employee education is key. It is all too easy to click on links like “check out this cool website!” or “install this antivirus software immediately.” Arming employees with knowledge will ensure they are aware of risks and the procedures to prevent an attack.

PASSWORD THEFT

Getting “hacked” through a compromised password/credential is a common occurrence that affects almost everyone at one time or another. However, it is much worse for a company because of the magnitude of damage that can be done through compromised sensitive data. Password theft attacks vary in technical complexity and cost, never leaving without lasting damage to its victim.

COMMON PASSWORD THEFT ATTACKS

Credential Stuffing

Using a database of compromised credentials, the hacker replays the data against the target system hoping that one of the credentials will match a legitimate user.

Password Spraying

Using a list of commonly used passwords, the hacker replays them in the hope that one will be used by a legitimate user.

Brute Force Attacks

After obtaining an encrypted blob that contains credentials of interest, the hacker then uses a computer rig to crack through the database until the passwords are revealed.

Phishing and Malware Attacks

By encouraging a user to click on a link or download a file containing malware, the hacker can use either an exploit kit or the malware to exfiltrate the users credentials.

PREVENTING PASSWORD THEFT

Aside from the obvious preventative measures (never share your password, don't use the same password for multiple accounts, and never use personal information in your passwords), there are two easily implemented steps that can protect your data from password theft.

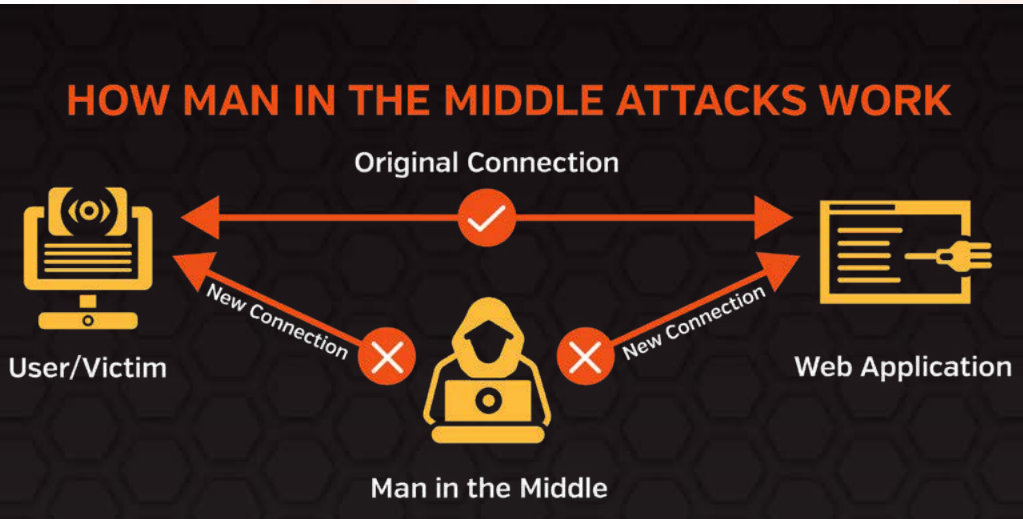
1. ***Multi-Factor Authentication:*** There is an increasing number of online services that offer multi-factor authentication to protect your sensitive information. Authentication will require an additional step between entering your password and accessing your account. Typically, the additional step is a code sent to the phone number you have on record. For those services that don't offer multi-factor authentication, there are also software applications available that serve the same functionality. Some of the most highly rated apps include: Duo Security, Authy, and Google Authenticator.
2. ***Password Manager:*** Password managers keep track of usernames and passwords for the various sites you use. In addition to securely storing your credentials in encrypted "virtual vaults," Password Managers offer randomly generated passwords for you to utilize, adding yet another level of security to prevent theft.

OTHER NOTABLE CYBERSECURITY THREATS

TRAFFIC INTERCEPTION OR MAN IN THE MIDDLE (MITM) ATTACKS

Traffic Interception, or Man in the Middle (MitM) Attacks, occur when an attacker intercepts communications between two parties. Using an interceptor software, the hacker redirects the encrypted connection to the interceptor which pretends to be the requested website. The interceptor then opens a new encrypted connection to the destination website. The interceptor acts as a proxy for the data between the two connections. Through this connection, the interceptor's access to the data is now unencrypted, so they can read, change, or block any of the content sent or received.

The best way to prevent Traffic Interception is to avoid compromised websites such as ones not using HTML5. When an HTTPS connection is established, the browser confirms the identity of the website by verifying the authenticity of the certificate presented by the web server. When a certificate fails the verification, a warning will alert the user that the connection is potentially insecure. If you notice that the lock is open adjacent to the URL address in the browser window, avoid using that website. Another preventive measure is to encrypt network traffic through a Virtual Private Network (VPN).

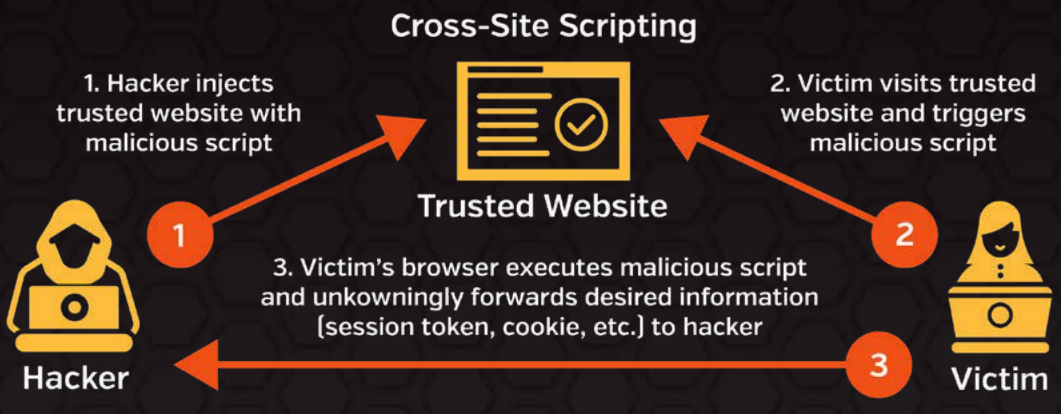


CROSS-SITE SCRIPTING ATTACKS (XSS)

Cross-Site Scripting Attacks, also known as an XSS attack, aim to either disrupt standard services or steal user information. The hacker injects malicious code into a web page that the intended victim visits. This code becomes a vehicle to deliver the attack to the victim when they visit that site. Vulnerable vehicles for Cross-Site Attacks include forums, message boards, and web pages that allow for comments. The actual attack occurs when the victim visits the web page or application which activates the malicious code.

From the host's side, encryption is usually required to prevent XSS attacks. Websites need to be kept updated and any vulnerabilities need to be corrected. There are software programs available that find and test for XSS vulnerabilities.

From the user's side, ensure that the company has a good antivirus software installed. Installing a firewall is an additional countermeasure. It is also crucial to have all equipment and software properly and consistently updated. Many of the XSS threats are based on vulnerabilities caused by failures in our equipment or software. Of course, common sense is critical. Don't visit sites that may be unsafe, such as ones accessed through third-party links that show something suspicious. Lastly, don't download files or install software from suspicious sites.



KNOW THE ENEMY

Cyber Attackers are constantly searching for new ways to breach security protocols to exploit companies. New threats will always be popping up. The key to protection is knowing the intent and tactics of cybercriminals, then ensuring that your company is taking all necessary precautions to thwart would-be attackers.

As they say, an ounce of prevention is worth a pound of cure.

COMPUTER DATA SECURITY AND NETWORK SECURITY FOR BUSINESS

If worrying over malicious cyber attacks is preventing you from moving forward, talk to the experts at FUSE3. We powerfully shield the vital information of your company with our total Computer Data Security Solutions so you can put your worries aside. Our Network and Data Security solutions, along with virus removal, malware, and spam protection services, protect your company from all that's out there.

GET A FREE AUDIT NOW

916-484-1780

FUSETHREE.COM | FUSE3