Cybersecurity Awareness Handbook

Sensei Enterprises, Inc.

Sharon D. Nelson, Esq., John W. Simek,
Michael C. Maschke, and Zachary C. Roush

Cybersecurity Awareness Training

Cybersecurity awareness training is critical. We recommend that a business offer mandatory cybersecurity awareness training at least once a year for all employees. Cybersecurity awareness training keeps employees aware of the ever-changing ways in which attackers may try to gain access to critical information and systems.

Cybersecurity awareness training can be tailored to your own needs as a business!

What is covered?

A lot of information is covered in cybersecurity awareness training. Common attack methods such as **Business Email Compromise (BEC)**, **Phishing, Smishing (phishing via texts)** and **Social Engineering** are discussed, as well as information about **passwords**, passkeys, **MFA**, **ransomware** and much more. Examples of real-life phishing e-mails and texts are critical training components.

It doesn't have to be dull — it can be engaging, informative, and most importantly, effective!

Business Email Compromise (BEC)

BEC is a type of attack that can cause significant financial damage to its victims. In these scams, criminals send an email message that looks like it has come from a known source – which makes it appear legitimate. Sometimes it looks like a message from the CEO or the Principal of the business asking to buy gift cards for employees - or maybe it asks an employee to transfer funds from the company account to another account to pay an invoice. Whatever it looks like, the attackers are only after one thing – money.

BEC Attackers May:

- Spoof email accounts or websites
- Send a targeted phishing email or text
- Use malware
- Compromise a valid email account

Social Engineering

Social engineering is the process of using deception to manipulate a target into revealing or divulging personal or confidential information that can then be used for fraudulent purposes.

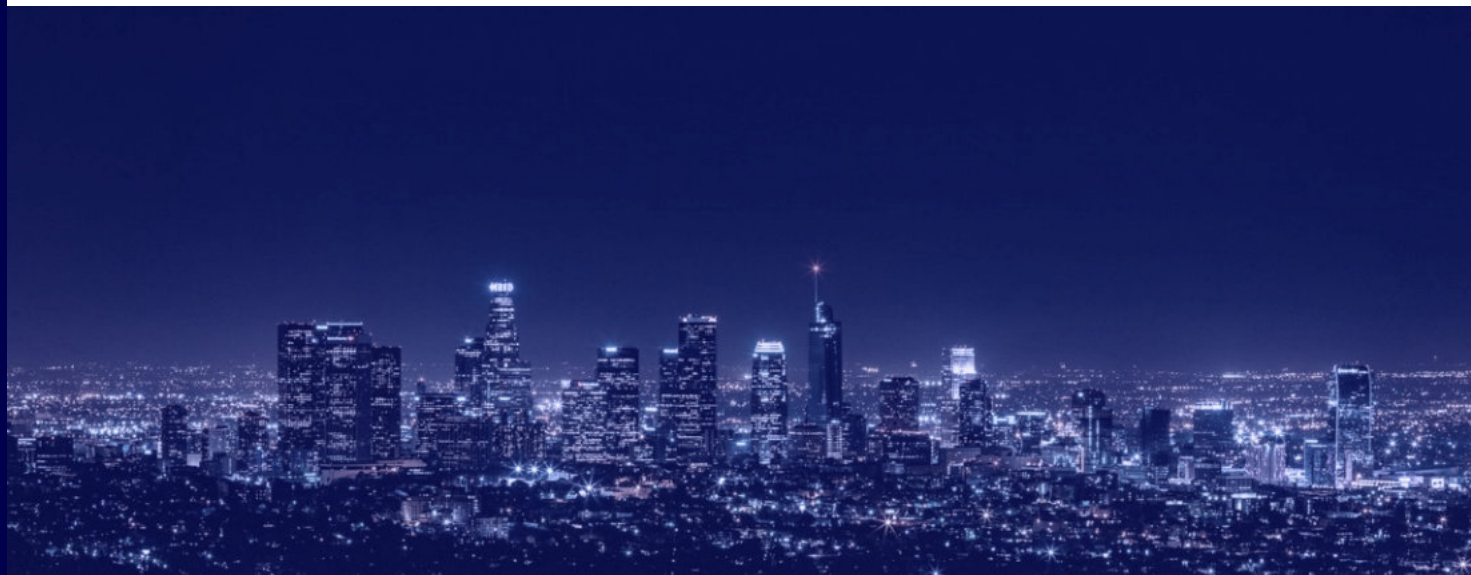
Phishing

Phishing is the practice of sending fraudulent communications purporting to be from a reputable source to convince individuals to supply personal information such as passwords and credit card information.

Whaling is aimed at high-value targets, CEOs and Principals of businesses.

Phishing Takes Several Forms:

- **Email**
- **SMS/Text Message (Smishing)**
- **Voice (Vishing)**
- **Spear Phishing (targeted), including Whaling**



Passwords

Strong passwords and PINS are used to keep sensitive data safe and secure.

Protecting Your Passwords

1. Don't write down passwords.
2. Don't share passwords
3. Don't reuse passwords
4. Create strong, complex passwords that you will remember, such as a passphrase
5. Use a password manager
6. Don't store passwords in your browser

If your passwords are stored in your browser and you're compromised, then an attacker has all your passwords plus the history of where they were used.

Zero Trust

ZERO TRUST SECURITY

Verify All Users

Validate User Devices

Limit User Access

Trust no one, verify everything

Reauthenticate users and devices periodically.

Multi-Factor Authentication (MFA)

What is MFA?

MFA adds a layer of security by requiring an additional method of verification - that is, multiple factors - during authentication.

USING MFA IS EASY AS 1,2,3.

The 3 Principles of MFA

1. **Something You Know**

   Usually a PIN, passcode or password.

2. **Something You Have**

   A real-time, unique code for verification or a hardware token such as a YubiKey.

3. **Something You Are**

   This can be a fingerprint, facial recognition, iris scan, or another type of biometric indicator.

Why use MFA?

MFA adds an additional layer of security to your accounts, helping to prevent unauthorized access. Often with MFA, you are prompted to set up MFA the first time you log into your account. Many vendors provide you with an option to set your computer or phone as a trusted device, so that you are not prompted for MFA every time you log into the account.

MFA & the big picture

MFA is not going away. Most organizations require it. Most cyberinsurance providers require the use of MFA for their policy holders.

Secure ways to use MFA

1. Use a hardware token.
2. Use push notifications, which you can simply accept.
3. Use an authentication app.
4. Have a code texted to phone.

Top Ten MFA Excuses

1. My password is strong enough.
Great! If you're using a strong password then you care about security. Implement MFA to add an additional layer!

2. I don't want to provide my personal smartphone number for my MFA sign-in.
There are other forms of authentication that can be used in place of SMS text messages, such as a mobile app or even a physical security key.

3. My personal phone number will be used for marketing or sold to third parties
Make sure that your IT (Information Technology) provider has privacy protections in place so that your data isn't sold to third parties or for marketing. On the other hand, without MFA, your account could be compromised and then attackers have your information.

4. MFA is too new, unproven, and expensive.
MFA has been around for several decades now, and it continues to add an additional layer of security to accounts and systems. If it is cost that worries you, MFA is generally free.

5. Our IT team is already overloaded with addressing higher-priority issues.
If an attack such as ransomware occurs, your IT team will be even more overloaded. MFA can be a preventative measure to prevent an attack.

Top Ten MFA Excuses

6. It's too much of a hassle to set up MFA
MFA can often be set up quickly—sometimes with a simple click of a button.

7. The MFA solution does not support our legacy applications
Check support for the MFA vendors out there—you may find that there is support now for some legacy applications.

8. The risk is not high enough for the investment in MFA
In the WFH and remote environments of the workforce today, MFA is almost a necessity when employees are accessing data from unsecured home or public networks.

9. I don't know enough about what MFA is to feel comfortable using it.
No problem, our consultants will explain it to you in an easy-to-understand way!

10. I don't need more security; I don't have anything worth stealing.
Yes you do. Attackers are after one thing - money. They will take anything they think will make them a profit. They especially like credit card numbers, banking information and SSNs.

Ransomware

What Is Ransomware?

Ransomware is a malicious program that encrypts data on a computer, server, smartphone, and more, rendering data inaccessible. The attackers then demand payment to provide you with the decryption key or more frequently, they promise not to publish or sell your sensitive data online.

Types of Ransomware Attack Methods

1. Malware
2. Email Attachments
3. Web Pages
4. Pop-ups
5. Instant Messages
6. Text Messages
7. Social Engineering

Endpoint Protection

What is Endpoint Protection?

Endpoint protection encompasses cybersecurity principles like installing antivirus software, using **Security Information and Event Management (SIEM)** tools or **Endpoint Detection & Response (EDR)** software to protect your systems.

What is EDR?

Endpoint Detection and Response (EDR) is an endpoint – also known as a computer, server, or mobile phone-security solution that monitors devices used by end-users. It detects, prevents and responds to advanced cyber threats, such as ransomware.

Ransomware & Malware Prevention Checklist

- □ *Use MFA*
- □ *Upgrade your router and firewall to include IDS/IPS functionality*
- □ *Keep software updated and patched*
- □ *Use strong, complex passwords and a password manager*
- □ *Install endpoint detection and response (EDR) software on all endpoints*
- □ *Require mandatory, annual cybersecurity awareness training for all employees*
- □ *Utilize a cloud backup service and keep backups secured and offline*
- □ *Implement phishing simulation tests for all employees*
- □ *Utilize WPA2 or WPA3 to encrypt wireless network traffic*
- □ *Change all factory default settings*
- □ *Implement inactivity timers on all devices*
- □ *Maximize log collection and retention*
- □ *Start implementing zero trust architecture (ZTA)*

Cybersecurity Assessments

What is a cybersecurity assessment?

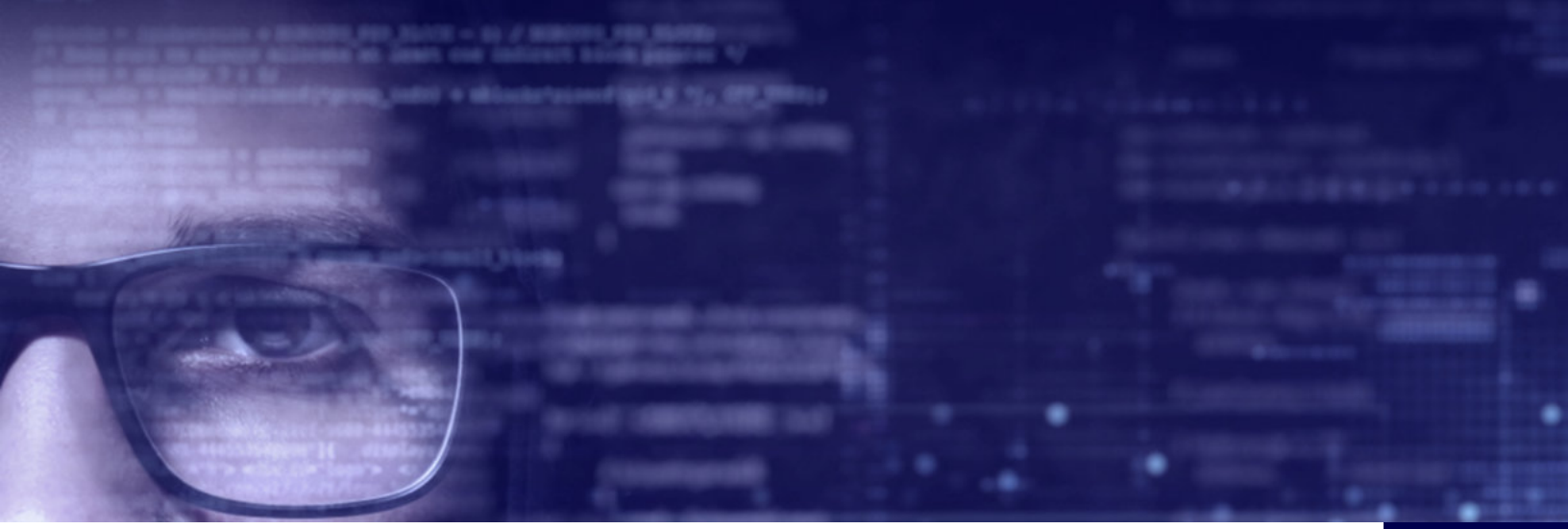
A security assessment analyzes your environment's current security posture and helps to identify weaknesses and vulnerabilities that can be exploited by threat actors. Once vulnerabilities are identified, remediation of those vulnerabilities can begin, starting with critical vulnerabilities.

The value of a cybersecurity assessment

Having a security assessment is key to determining if your company's infrastructure is properly prepared to defend against a wide range of threats. The goal is to identify gaps in your security so that they can be addressed and remediated. Cyberinsurance companies may require such assessments - so may customers and clients. Sensei offers a flat fee assessment (including the report) to simplify budgeting. Sensei also offers estimates to remediate and address any vulnerabilities that are discovered during the assessment.

Cybersecurity Assessment Steps:

1. Determine the scope of the assessment
2. Identify cybersecurity vulnerabilities
3. Review the security assessment report, address critical vulnerabilities first
4. Repeat the process at least annually



Intrusion Detection & Prevention Systems (IDS/IPS)

What is IDS/IPS?

Having an IDS or IPS is a great way to secure your network. These can be either stand-alone devices that you connect to your network, or they can be built into your firewall.

These devices scan your network traffic – the information entering and leaving your network. They analyze the traffic for signs of possible intrusion, attack methods or imminent threats to your network.

What are the benefits?

The IDS/IPS will monitor your network traffic and look for known malicious activity and behaviors. Attackers will try to compromise your network by exploiting vulnerabilities on a device or within software. The IDS/IPS can help find those vulnerabilities before an attacker exploits them and issue an alert. This allows you to block or patch the vulnerability so that attackers cannot gain access to your data.

Contact Sensei's CEO for more information.

Michael C. Maschke

mmaschke@senseient.com
https://senseient.com
703.359.0700

SENSEI ENTERPRISES, INC.

Your trusted provider of managed cybersecurity, information technology and digital forensic services.