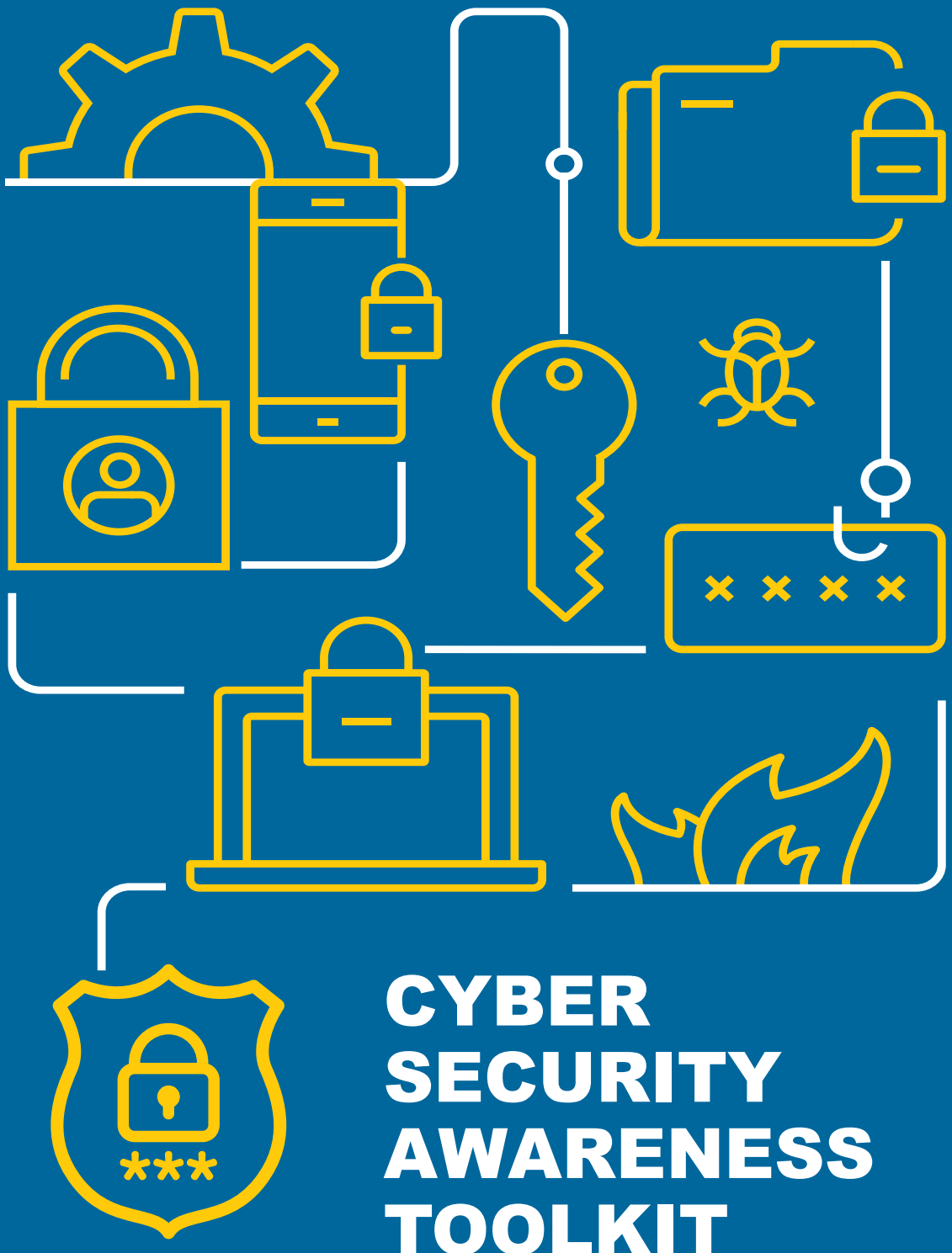
CHRISTIAN BROTHERS SERVICES



CYBER SECURITY AWARENESS TOOLKIT

Table of Contents

Introduction

How to use this toolkit

We developed this Toolkit to help your organization apply appropriate controls to manage cyber security threat situations. In addition, the documents aim to guide you in creating a training and awareness schedule for your staff. By using the Toolkit, you can create a planning process for your organization that will allow you to recognize and assess cyber threats. An included sample schedule will help you ensure your organization is taking the proper safety measures yearly for cyber security training and awareness. The Toolkit focuses on various types of cyber security including phishing, vishing, smishing, USB, tailgating, password protection, ransomware, and social engineering. It is our goal that this Toolkit will provide the most up-to-date knowledge on cyber security preparedness best practices to ensure your organization and its employees have a safe work environment.

Cyber Security Training and Awareness Schedule

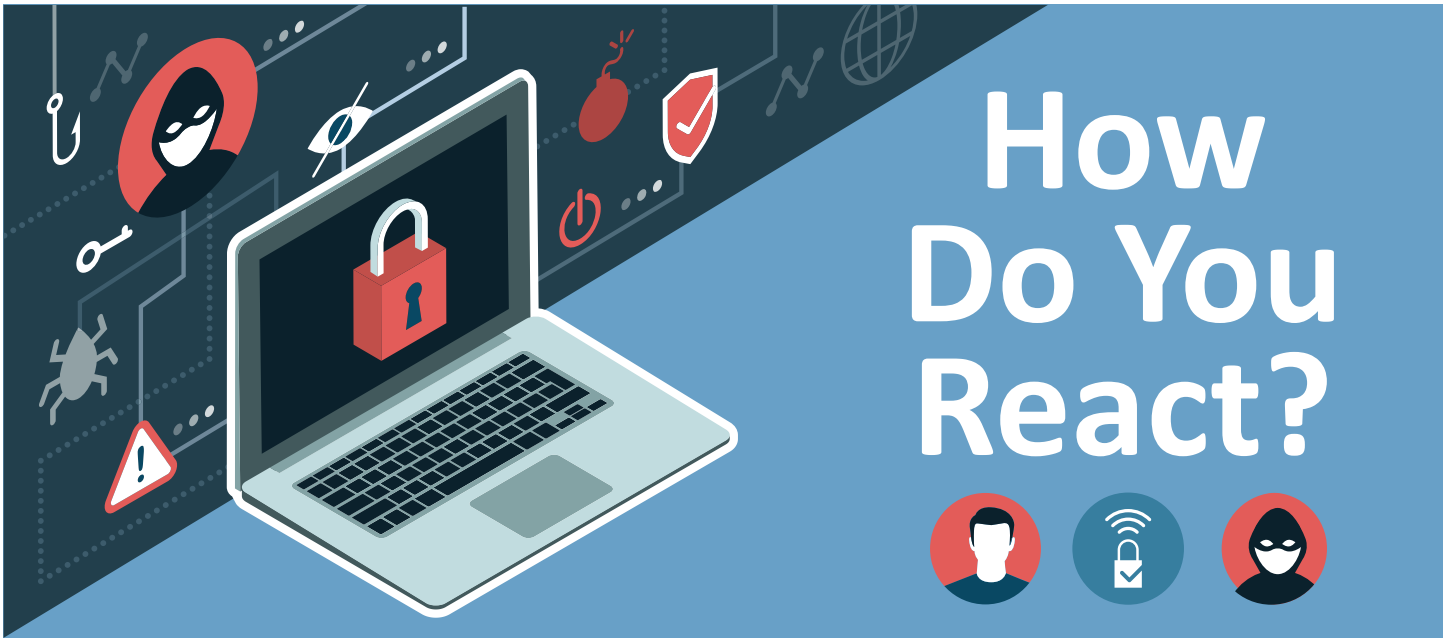
Can be completed monthly or quarterly over three years

	Dates	Training	Awareness
Q1	January	Assign Online Training Topic of Choice	Monthly Topic in Phishing
	February	Assign Online Training Topic of Choice	Monthly Topic in Vishing
	March	Assign Online Training Topic of Choice	Monthly Topic in Smishing
Q2	April	Assign Online Training Topic of Choice	Monthly Topic in USB
	May	Assign Online Training Topic of Choice	Monthly Topic in Tailgating
	June	Assign Online Training Topic of Choice	Monthly Topic in Passwords
Q3	July	Assign Online Training Topic of Choice	Monthly Topic in Social Media
	August	Assign Online Training Topic of Choice	Monthly Topic in Ransomeware
	September	Assign Online Training Topic of Choice	Monthly Topic in Social Engineering
Q4	October	Assign Online Training Topic of Choice	Monthly Topic in QR Codes
	November	Assign Online Training Topic of Choice	Monthly Topic in Passwords
	December	Assign Online Training Topic of Choice	Monthly Topic in Ransomeware

How to use:
Reference the table above as an example for monthly organization of cybersecurity topics. Assign the training early in the month and give a completion deadline by the end of the month to make consistent online training manageable for employees.

Members should update cyber security information for their program annually through CBS and/or internet resources.

This step should be delegated either to a responsible committee or to a specific person in order to ensure that a yearly schedule is produced, information is disseminated, and any possible training is assigned.



What is Social Engineering?

Attacks against computers, people, and mobile devices. The practice of convincing you to behave or reveal sensitive information by tricking or influencing you.

Types of attacks:

Digital

Phishing: Social engineering using email that targets an organization.

Spear Phishing: Social engineering using email that targets a specific person or position.

Your Defense: Examine the email to see if it appears suspect; if it does, do not click on any links or attachments; instead, report the email to the people in the organization in charge of preventing Cyber-attacks.

In-Person

USB Attacks: A hacking attack that infects your computer with malware by using a thumb drive.

Tailgating: When a hacker enters a building after an authorized person and gets past the physical entry barriers.

Your Defense: Deploying security entrances throughout your facility can help to ensure that your business data stays safe and protected, and that your risks are mitigated.

Mobile/Phone

Smishing: Texts that appear to be from trustworthy organizations sent to get people to divulge personal information, like passwords or credit card numbers.

Vishing: Phone calls or voicemails that appear to be from trustworthy organizations to persuade people to divulge private information, such as bank details and credit card numbers.

Your Defense: When a call or text asks for personal information or money on the phone and claims to be from a bank or a government organization, be suspicious. Never believe anybody who makes you feel as though you need to call them immediately. To be sure the contact is genuine, take a moment, conduct some research, and dial legitimate numbers.

Phishing

Email Attacks

Can You Identify the Phish?

People are still being extorted using phishing scams. Even if you are aware of what phishing is, 97% of people still struggle to recognize a phishing email. ***79% of U.S. organizations say they experienced a successful phishing attack in 2021!***

But it is not just organizations that are suffering. Individuals in their personal capacity are being targeted more and more. In 2022, 3.4 billion phishing emails were sent, making up almost 50% of total emails. Each month, the number of new phishing websites amounts to roughly 1,385 million.

79%

of U.S. organizations

say they experienced a successful phishing attack in 2021!

Ask Yourself These Phishing Questions

1

Is the message sent from a public email domain?
No legitimate organization will send emails from an address that ends "@gmail.com" or "@hotmail.com."

2

Is the email poorly written?
If an email has poor grammar and spelling, you can usually tell that it's a fraud. When using a spellchecker or translation tool, scammers frequently get all the correct words, but not always in the right context.

3

Does the email contain suspicious attachments or links?
Never open an attachment unless you are confident that the message is from a legitimate party. Train yourself to hover your mouse over every link before you click. The destination address appears in a small bar along the bottom of the browser.

4

Does the message create a sense of urgency?
Many scams request you act now, or else it will be too late. If an email pressures you to act quickly, it probably is a fake.

Vishing / Smishing

Over-the-Phone and Text-based Attacks

Beware of this Sophisticated Cyberattack!

When a cybercriminal attempts to persuade you into providing sensitive information over the phone, it is known as "voice phishing" or "vishing." The only step in typical vishing is a phone call. However, to further deceive their victims, scammers are now combining emails, texts and phone calls. This use of texting is called "smishing."

Here's a typical vishing/smishing scam scenario:

1. The victim receives a text or email appearing to be from a reputable organization (such as a bank, the IRS, a tech company, or a retail site) that claims there is a problem with their account or order.
2. The message instructs the victim to call a phone number to resolve the issue.
3. When the victim calls the number, a fraudster answers the phone and impersonates a representative of the organization.
4. The fraudster then asks the victim to provide sensitive information, such as their social security number, credit card number, or login credentials.
5. The scammer uses the information obtained to steal money or commit identity theft.

By combining texts, emails and phone calls, scammers can create a sense of urgency and authority to convince the victim to disclose sensitive information, which they then use for fraudulent activities.

What You Can Do

Watch for generic greetings.
Phishing emails and texts may use a generic greeting like "Dear Customer" instead of your name.

Keep track of your deliveries.
Scammers believe you'll presume without investigating that they're referring to a package you recently ordered. If you are aware of the packages you will be receiving, who will send them to you, and when, they will have a lot tougher time duping you.

From: Orders <GenericEmail@gmail.com>
To: John Doe
Subject: Your Order

Thanks for your order! It is being processed and will ship soon.

Order Date: 01/01/23
Payment Type: Credit Card
Amount Paid: $625.85

If you did not place this order, please call Customer Service at 888-###-#### within 24 hours to cancel.

Know delivery company policies.
Never allow delivery businesses to phone or text you without your permission. Messages are often posted inside a protected web portal, depending on how you signed up for alerts. Be wary of unauthorized communications, especially if you have never signed up for text alerts.

Never provide private information to a stranger.
Even if the caller claims to be from a firm you trust, if you get an unwanted request for personal information, hang up and dial the business's main customer care number. The simplest approach to assess if the enquiry is authentic or a scam is to make your own phone call to the business.

Never call the number in a suspicious email or text, even if you do business with the listed business. Call the customer support number listed on the company website to ask questions regarding the transaction described in the email or text.

Password Safety

How to Keep Your Passwords Safe

Passwords are a necessary evil, but one of the big problems with them is that you have too many. Passwords are also challenging to remember, unless you use the same one across the board, which is never a good idea.

Another password problem is security. Passwords can be stolen through system breaches, criticized for being too basic and easy to hack, or they are just too complex and convoluted to really remember. The truth is that hackers can easily steal personal information since password technology is so simple. But knowing how are they doing it can help you avoid becoming a victim of password theft.

Keeping up with the most recent password security techniques can leave your head spinning. The reality is that cybersecurity is always changing. However, keeping abreast of all the methods thieves employ to get access to your systems is a big part of maintaining your password safety.

Here are a few methods bad actors use to steal your passwords:

1. Phishing attacks

Phishing is one of the most common methods hackers use to steal personal information, including passwords. Phishing is when a hacker posing as a trustworthy party sends you a fraudulent email, hoping you will reveal your personal information voluntarily.

Avoid by:

- Protecting your computer by using security software. Set the software to update automatically so it will deal with any new security threats.
- Protecting your cell phone by setting software to update automatically. These updates could give you critical protection against security threats.
- Protecting your accounts by using multi-factor authentication. The extra credentials you need to log in to your account fall into three categories:
  - ► Something you know — like a passcode, a PIN, or the answer to a security question
  - ► Something you have — like a one-time verification passcode you get by text, email, or from an authenticator app; or a security key
  - ► Something you are — like a scan of your fingerprint, your retina, or your face
- Protect your data by backing it up. Back up the data on your computer to an external hard drive or in the cloud. Back up the data on your phone, too.

2. Credential Stuffing

This is a method hackers use to compare databases or lists of compromised credentials, such as user names and passwords, to various accounts to see whether a match exists.

Avoid by:
Make sure every password for every site is unique.

3. Malware

Malware is capable of anything from actively shutting down computers to deleting files to covertly tracking your activities. Keylogging malware will monitor the keystrokes entered onto a keyboard or keypad directly, enabling password theft. Webcams might be hacked by spy software to record and observe you.

Avoid by:
Using a firewall and installing and updating security software. Make sure that your operating system, web browser, and security software are all set to update automatically. Don't weaken the security settings on your browser.

4. Brute Force

Hackers that use this technique to run algorithms against an encrypted password until the algorithm decrypts it and displays the password in plain text.

Avoid by:
Making sure your passwords are long enough, 16 characters at minimum. Or use passphrases or biometrics, such as fingerprint or facial recognition in lieu of passwords.

5. Dictionary Attack

This type of brute force attack relies on our propensity to choose "simple" phrases as our passwords; the most popular of these terms have been compiled by hackers into "cracking dictionaries." More complex dictionary attacks include terms that are significant to you personally, such as your hometown, a child's name, or the name of a pet.

Avoid by:

- Creating unique passwords, ideally a combination of random words with symbols and numbers. Don't reuse or share them, and ensure they are changed if there is a compromise. A password manager can help ensure your passwords are unique.
- Setting up multi-factor authentication where possible.
- Limit the number of attempts allowed within a given period of time.
- Move away from short passwords and start using passphrases.

Passphrases vs. Passwords

Complicated passwords can lead to problems

Through the years, we have been told that using passwords which are lengthy, complicated, and even random provides us with the best security. Common sense tells us that a password's difficulty to guess would increase with its complexity. However, the use of overly complicated passwords can cause unintended consequences for both people and organizations.

With the sheer number of passwords we all use in our daily lives, even the most security-minded individuals can have a difficult time keeping track of all of them. That often leads to problems, such as:

Memorization: Lengthy, complex and random passwords can be difficult to remember, leading to the use of writing down or reusing passwords, both of which can compromise security.

Usability: Some systems have restrictions on password length or character types, making it difficult to use strong passwords everywhere.

Password Fatigue: Having to constantly create and remember unique, complex passwords for multiple accounts can lead to password fatigue and decreased security as users resort to weak passwords or reuse the same password across multiple accounts.

Passphrases instead of passwords

Hackers use a password cracker, which is a piece of number-crunching technology (or even a free software application or web service) that can decipher weak passwords in fractions of a second. According to the Center for Internet Security (CIS), a hacking program can crack a short password that is less than eight characters in less than three microseconds.

As password cracking technology has improved and grown more popular, it has become significantly more harmful to our data. What was once considered a safe password is now a piece of cake for hackers to slice through. According to TechRepublic, a 7-character password with letters, numbers and symbols would take seven minutes to crack in 2020 but just 31 seconds in 2022. That is why it is crucial to generate and manage secure passwords, particularly for key accounts such as financial and email accounts.

Instead of an overly complicated password, a better practice is to use random words in a passphrase. A passphrase is a long string of often random words, often more secure than passwords, but usually easier to remember. A passphrase is longer than a password and can contain spaces in between words, can contain symbols, and does not have to be a proper sentence or grammatically correct. Passphrases are difficult to crack through brute force, a hacking method that uses trial and error to crack passwords, login credentials, and encryption keys. Many password-cracking tools work to break down 10-character passwords. Since passphrases are longer, they can be much more secure and safe from these tools. But the phrase doesn't have to be impossible to remember. A simple password or passphrase that uses 12 upper and lowercase letters without any numbers would take a hacker 24 years to brute force. A password or phrase with 18 upper and lowercase letters, numbers and symbols would take a hacker an astonishing 438 trillion years to crack!

One of the simplest yet strongest passphrase choices is to just throw three or four random words together, like "courageous whale library." As long as it is at least 12 characters and the words are truly random without a natural flow to them, then this should make for a very strong passphrase. The best way to create a passphrase is to combine a group of words into a phrase that makes sense to you and is easily remembered, but makes no sense to anyone else. Memorize your passphrase by writing it down on a piece of paper. It should become second nature after a few applications. If you're having problems remembering, make a narrative out of it.

Passphrases that place a premium on simplicity are better than complex passwords for several reasons:

1. **Memorability:** Simple passphrases are easier to remember, reducing the likelihood of writing them down or using a password manager, which can compromise security.
2. **Length:** A long, simple passphrase can provide stronger security than a shorter, complex password. The length of the passphrase makes it more difficult for an attacker to crack.
3. **Usability:** Simple passphrases are easier to type, reducing the likelihood of typos, which can compromise security.
4. **Decreased Password Fatigue:** Using simple, memorable passphrases can reduce the burden of having to constantly create and remember complex passwords, leading to less password fatigue and increased security.

Overall, simple passphrases can provide a good balance between memorability, length, and security.

Password Manager Risk Management

Using a Password Manager

A password manager is a software program that can create, save, and sync login information between various devices. There are numerous choices, each with a few minor differences in features and price ranges.

What is a password manager?

A password manager is a tool that securely stores and manages login credentials, such as username and passwords, for various websites and applications. It uses encryption and secure storage to protect this sensitive information. When the user needs to log into a website, the password manager can automatically fill in the login form, saving time and reducing the risk of password reuse.

Follow organizational guidelines at work

Using a password manager at work is a good practice. By generating strong, unique passwords for each account, a password manager may help improve security while lowering the likelihood of data breaches. However, keep in mind that every organization is different and you should follow the guidelines put in place.

Consider a password manager for personal use

Using a password manager for personal use simplifies the process of accessing and managing passwords, making it easier to stay organized and reducing the risk of password-related headaches.

Password manager security

Password managers are generally considered to be secure, but the security of a password manager depends on its implementation and the security measures it has in place. To ensure the security of your password manager, it's important to choose one from a reputable provider and follow best practices, such as using a unique and strong master password, enabling two-factor authentication, and keeping your software up-to-date.

It's also important to note that no system is completely foolproof and password managers can be vulnerable to security threats, such as hacking or data breaches. However, when used properly, password managers can be a more secure option compared to reusing passwords or storing them in unencrypted files.

Education and Ongoing Awareness Training

Recognizing Cybercriminal Tactics

As technology continues to play a greater part in our everyday lives and business operations, cybersecurity is becoming more and more crucial. Employees are often an organization's first line of defense against cyberattacks, therefore, it's critical that they comprehend the tactics employed by hackers to safeguard both themselves and the organization.

Here are some of the most common tactics used by cybercriminals and what employees should look for to identify them:

1. **Phishing Scams:** Phishing is a tactic used by cybercriminals to trick individuals into providing sensitive information, such as passwords and financial information.

   Employees should be wary of emails or messages that ask for personal information, especially if they are from an unknown sender. It's also important to look out for emails with suspicious links or attachments, as these can contain malware.

2. **Malware:** Malware is any software designed to harm or disrupt computer systems. It can come in many forms, including viruses, Trojan horses, and ransomware.

   Employees should be cautious when downloading or opening attachments, especially from unknown sources. It's also essential to keep anti-malware software up to date to protect against the latest threats.

3. **Social Engineering:** Social engineering is a tactic that leverages human emotions and behavior to trick individuals into giving up sensitive information. For example, a cybercriminal may pose as a technical support representative and ask for access to a computer or sensitive data.

   Employees should be cautious of unsolicited requests for information or access and should verify the identity of anyone claiming to be from a technical support team.

4. **Password Exploitation:** Weak passwords are a common vulnerability for cyberattacks.

   Employees should create strong passwords that are at least 12 characters long and include a mix of letters, numbers, and symbols. They should also avoid using the same password for multiple accounts, change their passwords regularly, and enable two-factor authentication whenever possible.

5. **Man-in-the-Middle Attacks:** In a man-in-the-middle attack, the attacker intercepts communications between two parties and can eavesdrop on or modify the data being transmitted. This can occur when an attacker positions themselves between a victim and a legitimate website or service, and can be used to steal sensitive information or manipulate transactions.

   Employees should check that websites and applications they are using have HTTPS or SSL/TLS connections for sensitive online transactions to prevent eavesdropping.

6. **Mobile Device Attacks:** Mobile devices, such as smartphones and tablets, are becoming increasingly common in the workplace. However, they can also be vulnerable to cyberattacks, especially if they are not properly secured.

   Employees should ensure their mobile devices have strong passwords and keep them updated with the latest security patches.

7. **Public Wi-Fi:** Public Wi-Fi networks can be vulnerable to cyberattacks, as they may not be secure.

   Employees should avoid using public Wi-Fi to access sensitive information and should use a virtual private network (VPN) instead. A VPN encrypts internet traffic and helps protect against cyberattacks.

8. **Physical Security:** Employees should be cautious about leaving their devices unattended and should lock their computers when they are not using them. They should also be mindful of who is around them when entering sensitive information, as someone may be watching over their shoulder.

   Understanding and defending against cybercriminal tactics is critical for employees and organizations alike. By following the best practices outlined above, employees can help protect themselves and their organizations from cyberattacks. It's essential to stay vigilant and continually educate ourselves on the latest threats to stay protected.

Cybercrime is a costly expenditure for organizations.
The average cost of a data breach in the United States in 2022 was $9.44 million, according to IBM data.

Cybersecurity Ventures predicts cybercrime will cost businesses $10.5 trillion annually worldwide by 2025.

Education and Ongoing Awareness Training

Recognizing and Responding to Cybercriminal Attacks

Cybersecurity is a crucial aspect of modern business operations, as cybercriminal attacks can result in data breaches, loss of sensitive information, and damage to an organization's reputation. Employees play a vital role in helping to protect a company from these types of attacks. What can you, as an employee, do to recognize and respond to cybercriminal attacks? Here are some best practices:

- **Be wary of suspicious emails:** Email is one of the most common methods used by cybercriminals to launch attacks. Be cautious of emails that contain attachments or links, especially if they are from unknown sources or if the content seems suspicious or out of character for the sender. Before clicking on any links or downloading attachments, hover over them to see the actual URL and verify that it is from a trustworthy source.
- **Keep software and systems updated:** Regularly updating software and systems can help prevent cybercriminal attacks, as these updates often contain patches for known vulnerabilities. Ensure that all software, including your operating system, web browsers, and anti-virus software, are up-to-date and that you have installed all critical security updates.
- **Report suspicious activity:** If you suspect you have been targeted by a cybercriminal attack, report it immediately to your IT department. Do not ignore the problem, as it could lead to more serious consequences for both you and your company.
- **Be cautious when sharing personal information**: Be careful about the personal information that you share online, as cybercriminals can use this information to steal your identity or launch attacks. Avoid posting sensitive information on social media, and never share your passwords, social security number, or other sensitive information in emails or online forms.
- **Use caution when downloading software or files:** Downloading software or files from untrusted sources can result in your computer being infected with malware or other malicious software. Always download software or files from trusted sources, and verify the authenticity of any software or files before installing or opening them.
- **Back up important data:** Regularly backing up important data can help you recover from a cyberattack and minimize the potential damage. Store backup copies of critical data in a secure, offsite location and ensure that they are encrypted to protect against unauthorized access.
- **Be vigilant:** Stay alert and aware of your surroundings, and be mindful of the activities and actions of others when using technology. Be suspicious of unexpected emails, pop-ups, or alerts, and be cautious about providing personal information online.
- **Keep up to date on education:** Finally, it's essential for employees to have continual access to education about the latest cyber threats and tactics. Cybercriminals are constantly developing new ways to attack, and employees must stay informed to stay protected. Organizations should provide regular training sessions and resources for employees to stay up to date on the latest cyber threats.

Christian Brothers Risk Management Services provides online Cyber training modules designed to raise employee awareness to the tactics used by cybercriminals. Modules include:

- Cyber Email Security
- Cyber Internet Security
- Cyber Malware
- Cyber Password Security
- Cyber Phishing Prevention
- Cyber Remote Work
- Cyber Removable Media
- Cyber Social Engineering

Recognizing and responding to cybercriminal attacks requires a combination of technical expertise and vigilant awareness. You can help protect your company from these types of attacks and minimize the potential harm that they can cause. Cybercrime is a dynamic and evolving threat, and it is important to stay informed and up-to-date on the latest trends and best practices in cybersecurity.

What is it, where does it come from, and what are its effects

The increasing use of technology in today's world has made it easier for criminals to exploit data and spread misinformation.

Misinformation is false or inaccurate information that is spread deliberately to deceive people. It is a powerful tool that can be used to manipulate public opinion, influence decisions, and even create chaos and destruction. In the digital age, cybercriminals have leveraged misinformation and fake news to their advantage by using it to exploit data and steal sensitive information from individuals and organizations.

More and more, cybercriminals exploit data using misinformation through phishing attacks, which are designed to trick individuals into revealing their personal information, such as passwords and credit card numbers, by posing as a trusted entity. Cybercriminals often use phishing emails or fake websites to lure individuals into revealing their sensitive information. For example, an attacker may create a fake login page for a popular website, such as a bank or e-commerce site, and send emails to users asking them to log in to the fake page. Once the user enters their information, the attacker can then use it to steal their identity or access their accounts.

Cybercriminals also exploit data using misinformation through a variety of social engineering techniques. This involves manipulating individuals into divulging sensitive information or performing actions they wouldn't normally do. For example, a cybercriminal may create a fake social media profile posing as a friend or acquaintance and send messages asking for sensitive information. They may also use tactics such as fear or urgency to convince individuals to reveal their information, such as claiming there has been a security breach and they need to update their password immediately.

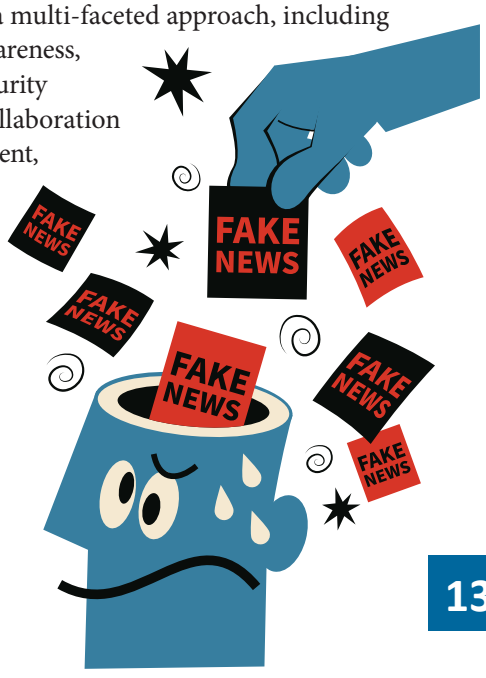
These social engineering scams are constantly changing and have become more and more sophisticated and more difficult to detect. Here are three examples of social engineering using misinformation that cybercriminals use to steal data from unsuspecting victims:

- **Impersonation scams:** Criminals may pose as a company representative or trusted third party and contact employees, asking them to provide sensitive information or access to data.
- **Baiting:** This involves leaving a device, such as a USB drive, in a public place with a tempting label on it, such as "confidential." When an unsuspecting employee inserts the device into their computer, it can install malware that provides the attacker with access to the company's data.
- **Pretexting:** This involves creating a fake scenario or pretext to obtain sensitive information from an individual or organization. For example, an attacker might pretend to be an employee from the IT department and call an employee, asking for their password under the guise of fixing a technical issue.

Cybercriminals also use misinformation to spread malware and other malicious software. They may create fake software updates or send emails with attachments that contain malware. Once the user downloads the malware, it can give the attacker access to their device and any sensitive information stored on it. Cybercriminals also may use fake advertisements to lure individuals into downloading malware disguised as a legitimate app or software.

It is important for individuals and organizations to be aware of these tactics and take steps to protect themselves, such as being cautious when revealing sensitive information, keeping their software up-to-date, and verifying information before taking any actions.

Additionally, it is important for society as a whole to work together to address this problem and find ways to diminish the impact of misinformation and cybercrime. This will require a multi-faceted approach, including education and awareness, stronger cybersecurity measures, and collaboration between government, organizations and individuals.



How employees can combat misinformation and fake news

Because of the development of technology and our growing reliance on the internet, cybercrime now poses a serious threat to both organizations and individuals. Misinformation from cybercriminals can have devastating effects on both a company and the individuals within it.

For several reasons, not the least of which is preserving the organization's reputation, it is crucial for workers to contribute to halting the spread of false information and rumors about their company. Misinformation can damage the reputation of a company, which can lead to a loss of business and revenue, which affects whether employees can keep their jobs.

For employees, being on the alert for, and stopping the dissemination of misinformation, can make the workplace a better place by:

- **Maintaining credibility:** Companies that are seen as trustworthy and credible are more likely to retain customers, employees, and investors.
- **Promoting a positive workplace culture:** A workplace culture that values accuracy, truth, and transparency can promote teamwork, trust, and open communication.
- **Fostering a sense of responsibility:** Employees who take responsibility for the accuracy of the information they share can contribute to a sense of ownership and pride in their work.
- **Upholding ethical standards:** Ethical standards require honesty and truthfulness in communications, and employees who help stop the spread of fake news and misinformation are upholding these standards.

As an employee, you are on the front line for spotting and halting misinformation, but what can you do to combat its spread? Here are some ways:

1. **Verify the source** of any information before sharing it with others. Make sure that the source is reliable and trustworthy.
2. **Check the facts** regarding the information you receive before sharing it with others. Use only reputable sources to confirm the accuracy of the information.
3. **Educate yourself** about misinformation and fake news. Learn how to spot fake news and understand the impact it can have.
4. **Use critical thinking skills** to evaluate information. Question the validity of information and think critically about the evidence.
5. **Avoid sharing unverified information** that you cannot verify. Only share information that you know is accurate and reliable.
6. **Report misinformation** or fake news you come across in the workplace. Alert your supervisors or HR representatives so that they can take appropriate action.
7. **Lead by example** by being responsible and ethical in your own communication and behavior. Strive to help create a workplace culture that values accuracy, truth, and transparency.
8. **Respond quickly** if you encounter misinformation about your company. Address the issue head-on and provide accurate, credible information to counteract the misinformation.
9. **Stay vigilant** by continuously monitoring your online presence and be prepared to respond to any new instances of misinformation as they arise. The spread of false information can be persistent, so it's important to remain vigilant and stay ahead of the curve.

Learning how to identify misinformation and fake news can not only protect the organization and ministry that you serve, it can also have a positive affect at home and your personal life. By taking these steps, you can contribute to halting the spread of false information about your organization, safeguarding its integrity and, perhaps, your employment.

Inside Ransomware

Ransomware Basics

You probably have heard about ransomware, but you may not know exactly what it is, how it works, or what can be done about it. Ransomware attacks are increasing in frequency, with the repercussions growing more severe than ever.

Ransomware is a type of malicious software (malware) that encrypts a victim's files or locks them out of their own computer or network until a ransom is paid. In other words, it is a form of extortion where cybercriminals demand payment in exchange for restoring access to the victim's files or devices.

Ransomware attacks typically begin with a phishing email, a compromised website or a vulnerability in a software system. Once the malware has infected the victim's system, it will encrypt files, making them inaccessible to the victim. The attackers will then display a message to the victim, typically demanding payment in cryptocurrency for the decryption key to unlock the files.

Types of Ransomware

Although there are countless strains of ransomware, they mainly fall into two main types: crypto-ransomware and locker ransomware.

- Crypto-ransomware is the most common type and encrypts the victim's files, making them inaccessible until the ransom is paid.
- Locker ransomware locks the victim out of their own computer or network, making it impossible to access any files or applications until the ransom is paid.

The Costs of Ransomware

Ransomware attacks can have devastating consequences for individuals and organizations alike. Besides the financial cost of paying the ransom, victims may also suffer from lost data, disrupted business operations, and damage to their own and their organization's reputations. The attackers may also steal sensitive information from the victim's system, such as financial data or intellectual property, which can then be used for further cybercrime or sold on the dark web.

To protect against ransomware attacks, it is important for employees to follow basic cybersecurity best practices:

- Keep software up to date.
- Use strong and unique passwords.
- Be cautious of suspicious emails or messages.
- Back-up important files regularly and keep the backup in a secure location, such as an offline or cloud-based storage system.

If you suspect you have become the victim of a ransomware attack at work, it is important that you alert your organization's IT department immediately.

Ransomware is a serious and growing threat to individuals and organizations. By following basic cybersecurity best practices and seeking professional help when needed, it is possible to protect against ransomware attacks and minimize their impact.

Avoiding Ransomware

To avoid becoming a victim of ransomware, employees can take several steps to reduce their risk of falling prey to these attacks.

Here are some tips for employees to avoid ransomware attacks:

1. **Don't click on links in suspicious emails:** Ransomware attacks often use social engineering tactics to trick users into clicking on malicious links. They often begin with a phishing email that contains a malicious link or attachment. These emails may appear to be legitimate, and they can be very convincing. Be wary of emails that contain links, especially if they are from an unknown sender, look suspicious, or contain urgent or threatening language, as these may be a tactic used by cybercriminals to pressure victims into taking action.
2. **Keep your software up to date:** Ransomware attacks often exploit vulnerabilities in software systems to gain access to a victim's files or devices. To mitigate these vulnerabilities, software companies often release updates that address security matters. By keeping software up-to-date, employees can ensure that any security vulnerabilities are patched and their systems are better protected against ransomware attacks.
3. **Use strong passwords:** Strong and unique passwords are critical to avoid ransomware attacks. Employees should avoid using the same password across multiple accounts or using easily guessable passwords such as "password123," your name, or date of birth. Strong passwords should include a mix of uppercase and lowercase letters, numbers, and special characters. It is also important to change passwords regularly and use multi-factor authentication whenever possible to add an extra layer of security to login credentials.
4. **Use antivirus software:** Install and use antivirus software on your personal computer, and use the antivirus software provided by your organization on your work computer. This software can help detect and remove malware, including ransomware.
5. **Backup your data regularly:** Regularly back up your important files and data to an external hard drive or cloud-based storage service. In the event of a ransomware attack, having a backup of your data can help you recover your files without having to pay a ransom.
6. **Be vigilant and report any suspicious activity:** Report any suspicious activity or messages to your IT department or manager. Prompt reporting can help prevent a ransomware attack from spreading throughout an organization.
7. **Be cautious about what you download and install on your devices.** Many ransomware attacks are spread through malware hidden in seemingly innocent software downloads or updates. Employees should only download and install software from trusted sources, and avoid downloading or installing software from unknown or unverified sources.

By being vigilant about emails, keeping software up to date, using strong and unique passwords, backing up important files, and being cautious about downloads and installations, employees can reduce their risk of falling prey to ransomware attacks. It is also important to stay informed about the latest ransomware threats and to seek help from cybersecurity experts if an attack does occur.

Ransomware Prevention and what to do if you are Attacked

Like it or not, employees are often the weakest link in an organization's cybersecurity, and many ransomware attacks occur because of human error or negligence. One of the most effective ways to reduce the chances of a ransomware attack is for employees to participate in an ongoing awareness training program provided by their organization. By educating employees on the risks and best practices associated with ransomware, companies can empower their workforce to be more vigilant and proactive in protecting against these types of attacks.

Awareness training helps reduce the chances of a ransomware attack by teaching employees how to identify and avoid phishing emails and other social engineering tactics commonly used by cybercriminals to spread ransomware. This includes training on how to spot suspicious emails or messages, how to verify the authenticity of links and attachments, and how to report any suspicious activity to IT or security personnel.

Ongoing employee awareness training can also help educate employees on the importance of keeping software and security systems up-to-date, regularly backing up data, and avoiding risky online behavior, such as visiting unsecured websites or downloading unauthorized software.

By instilling a culture of cybersecurity awareness and responsibility, organizations can significantly reduce the risk of a ransomware attack. This training will better protect you, as an employee, as well as your organization's customers and sensitive data.

You are the victim or a ransomware attack. Now what?

Chances are, you will face a ransomware attack at some point, so the key is to make sure you know what to do when it happens. Even with continued training, as long as there is a human element involved, there will always be a chance a ransomware attack succeeds.

If the worst has happened and you have fallen victim to a ransomware attack, what do you do? If you are hit, or you suspect you are a victim of a ransomware attack, here are some steps you should take as an employee:

1. **Immediately report the incident to your IT or security team:** Notify your IT or security team as soon as possible so they can investigate the situation and take necessary measures to contain the attack. If you do not have an IT or security team, contact your supervisor or manager immediately.
2. **Disconnect from the network:** If possible, disconnect your computer from the network or shut down your computer to prevent the spread of the ransomware to other devices on the network.
3. **Do not engage with the attackers:** It's important not to engage with the attackers or pay the ransom, as it will only encourage them to continue their malicious activities.
4. **Preserve evidence:** If you can, take screenshots or notes of any messages or notifications related to the ransomware attack. This information may be useful to your IT or security team in determining the scope and severity of the attack.
5. **Follow any instructions provided by your IT or security team:** Your IT or security team may provide specific instructions for you to follow in order to contain the attack and prevent further damage.
6. **Be patient:** Recovering from a ransomware attack can take time. Be patient and follow the instructions provided by your IT or security team. They will work to restore your systems and data as quickly as possible.
7. **Learn from the incident:** After the attack has been resolved, take some time to reflect on what happened and consider how your device was infected with ransomware so you can prevent the same thing from happening again.

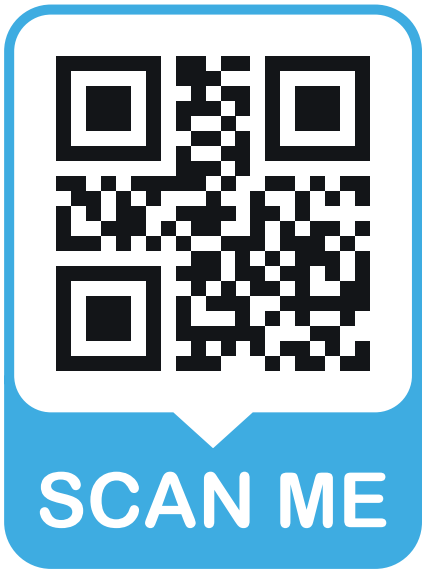
Don't wait until you're the victim of a ransomware attack to improve your cyber security awareness. Avoiding a ransomware attack in the first place through ongoing training and continued diligence is the greatest defense against one.

Avoiding Malicious QR Codes

QR codes offer a quick and easy way to access information or complete transactions. Unfortunately, malicious QR codes are also becoming more common, as hackers use them to spread malware or steal sensitive information. As an employee, it's important to be aware of the risks and take steps to protect yourself and your organization. Here are some tips to help you avoid malicious QR codes.

1. **Be cautious when scanning QR codes from unknown sources**
   One of the easiest ways for hackers to spread malicious QR codes is to place them on fake websites or in phishing emails. It is essential to be cautious when scanning QR codes from unknown sources. Before scanning a code, make sure that you trust the source and assure that it is a legitimate way to access the information you need. If you're not sure, it's better to avoid scanning the code altogether.
2. **Check the URL before scanning a QR code**
   Another way to protect yourself from malicious QR codes is to check the website's URL before scanning a code. Hackers often use QR codes to redirect users to fake websites, where they can steal sensitive information or install malware. Before scanning a code, make sure that the URL matches the website you were expecting to visit. If it doesn't, it is likely a malicious QR code and you should avoid scanning it.
3. **Use a QR code scanner with built-in security features**
   Some QR code scanners will automatically check the URL of the code and alert you if it is suspicious or potentially malicious. Others may use machine learning algorithms to detect patterns or anomalies in the code and flag them as potentially harmful. By using a scanner with built-in security features, you can reduce your risk of falling victim to a malicious QR code.
4. **Don't enter sensitive information after scanning a QR code**
   Another way that hackers use malicious QR codes is to trick users into entering sensitive information, such as login credentials or credit card numbers. To protect yourself, avoid entering any sensitive information after scanning a QR code, unless you're absolutely certain that it is a legitimate request. If you're unsure, it is better to err on the side of caution and avoid entering any information at all.
5. **Keep your device's software up-to-date**
   Finally, it's important to keep your device's software up-to-date in order to protect yourself from malicious QR codes. Hackers often exploit vulnerabilities in outdated software to spread malware or steal sensitive information. By keeping your device's software up-to-date, you can reduce your risk of falling victim to a malicious QR code.

As hackers continue to use malicious QR codes to spread malware or steal sensitive information, it is important for you, as an employee, to be aware of the risks and take steps to protect yourself and your organization. By being cautious, using good judgement, and following the tips outlined above, you can reduce your risk of falling victim to a malicious QR code.



CHRISTIAN BROTHERS SERVICES

Risk Management Services

1205 Windham Parkway • Romeoville, IL 60446
Anthony Chimera (*Risk Control Specialist*)
800.807.0100 x2512 • anthony.chimera@cbservices.org

3/2023