Outsmarting Online Scammers

Social Engineering: How Cyber Scams Deceive Us

Cybercriminals get our information by persuading us to share it. Online scammers trick people into revealing information they wouldn’t usually share. Instead of directly hacking devices, they use *"Social Engineering"* to manipulate individuals to provide the information they need.

How Does Social Engineering Work?

1. Cybercriminals utilize search engines and social media to collect information about individuals and businesses.
2. They often send messages that appear to originate from friends, family, or reputable companies.
3. These interactions can trick you into disclosing sensitive information, such as passwords, financial details, or personal data.

Keep Your Information Safe

- Limit what you share on social media
- Use different passwords for each account
- Be vigilant for signs of phishing

- ***Phishing*** is a type of cyberattack in which emails or messages look like they come from trusted sources. The goal is to fool people into sharing sensitive information, such as passwords, credit card numbers, or personal details.

Social Media Scams

Social media platforms, with billions of users, are prime targets for fraudsters due to the vast personal information shared by users. Cybercriminals exploit these vulnerabilities through fake profiles and phishing techniques to steal sensitive data. They often gather information from these platforms to launch targeted attacks, leading to identity theft and financial fraud. Additionally, the rapid spread of misinformation and malware on these platforms poses significant cybersecurity risks, highlighting the need for users to stay alert.

- ***Malware*** is a category of software programs designed to damage or do other unwanted actions to a computer system.

Social Media Scams to Watch Out For:

1. Investment and Cryptocurrency Scams: These scams offer fake opportunities to invest or get involved in cryptocurrency, promising high returns and no risks. Scammers trick victims into sending money or sharing personal information.

- ***Cryptocurrency*** is a type of digital money that uses cryptography for security.
- ***Cryptography*** is the study of ways to keep communication and data safe from unauthorized access or changes.

2. Fake Online Stores: Scammers set up fake online stores that look like popular brands and offer amazing deals. Victims end up receiving poor-quality products or nothing at all.

3. Romance Scams: Scammers create fake profiles to establish phony relationships and build trust with their victims, only to manipulate that trust to steal their money.

4. Job Scams: Fake job offers are common on social media platforms. These scams often ask for an upfront fee for training materials or background checks.

5. Survey and Quiz Scams: These scams encourage users to share personal information with the promise of rewards, often resulting in identity theft.

6. Tech Support Scams: Scammers pretend to be tech support and claim your device has a problem. They may try to gain remote access or convince you to pay upfront to fix a problem that doesn’t exist.

Phishing

The rise in phishing emails and smishing messages has increased the number of successful attacks, and this practice affects not only individuals but also organizations.

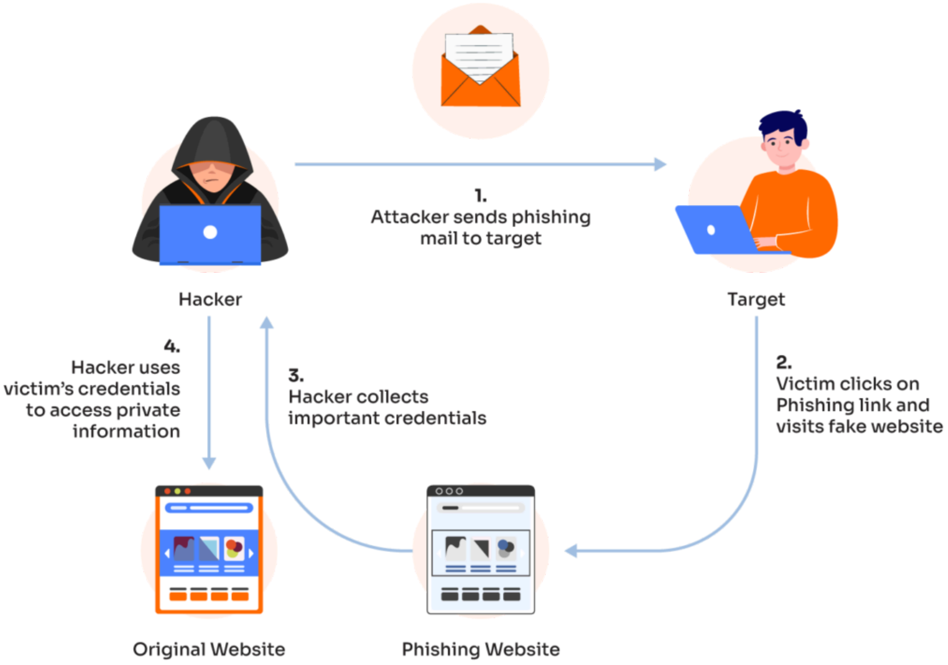
Security scans show that:

- *12% of phishing attacks deliver malware.*
- *Almost half (45%) of phishing attacks that ask for your login information wrongly claim to be from Microsoft.*
- *17% of phishing attacks are themed around finance.*

What are phishing emails?

It involves impersonating companies, organizations, or charities through emails. These emails often direct potential victims to click on a link, enter personal information, or make a payment. Cybercriminals gain access to sensitive information, including passwords that users believe have been validated in a legitimate system. This stolen information can then be used to carry out further scams.

The cycle of a phishing attack


1.
Attacker sends phishing mail to target
Hacker
Target
4.
Hacker uses victim's credentials to access private information
3.
Hacker collects important credentials
2.
Victim clicks on Phishing link and visits fake website
Original Website
Phishing Website

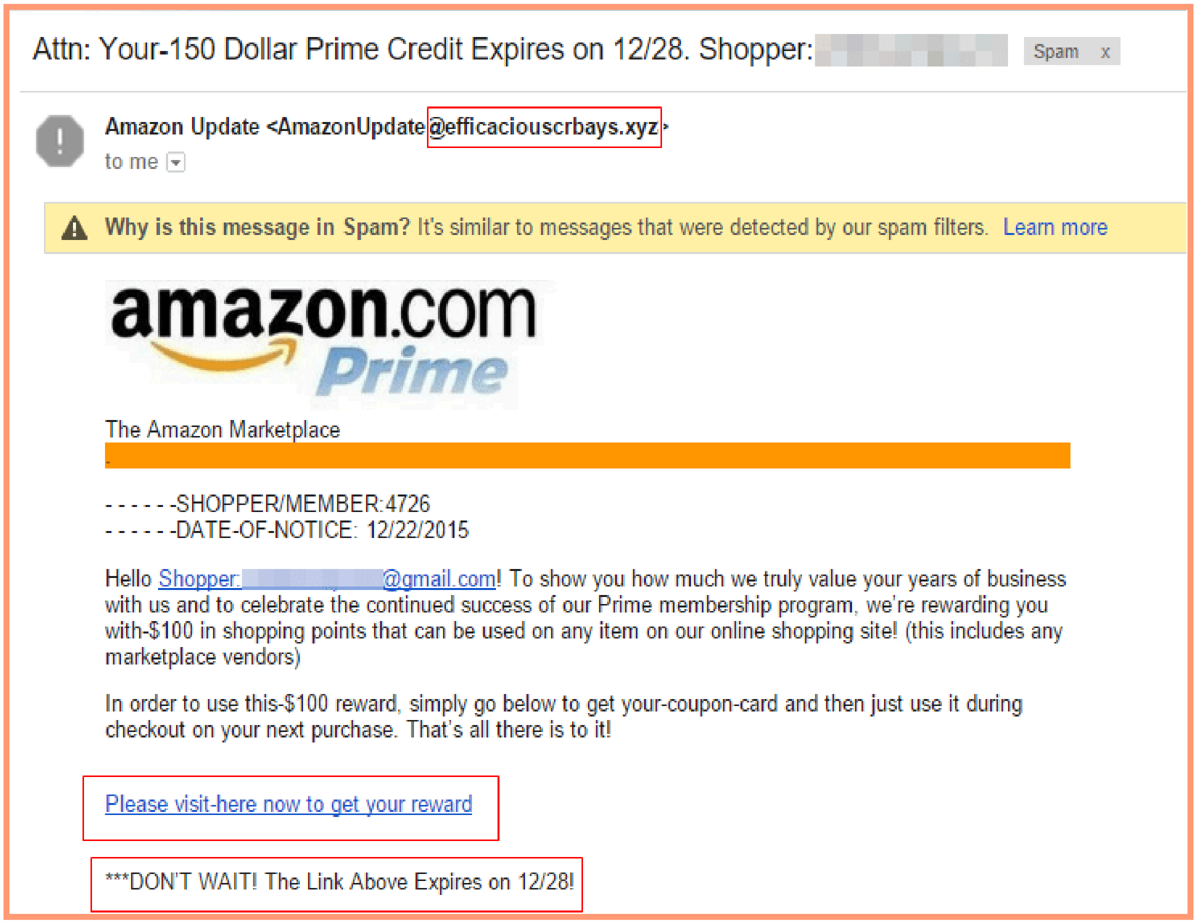
➢ ***A phishing website*** is a malicious site designed to look legitimate and trick users into providing sensitive information, such as usernames, passwords, credit card numbers, or other personal data. These websites often imitate well-known companies, financial institutions, or government agencies to gain the user's trust.

→ Signs of a phishing attack include but are not limited to:

1. Email addresses that don't match the sender's name.
2. Generic greetings.
3. Urgent or threatening language in the message.
4. Requests for personal information that you did not initiate.
5. Strange links or phrases like: "click here."

Example of Email Phishing Content

Can you spot the signs?



Attn: Your-150 Dollar Prime Credit Expires on 12/28. Shopper: [redacted]

Amazon Update <AmazonUpdate@efficaciouscrbays.xyz>

to me

Why is this message in Spam? It's similar to messages that were detected by our spam filters. Learn more

The Amazon Marketplace

- - - - - -SHOPPER/MEMBER:4726
- - - - - -DATE-OF-NOTICE: 12/22/2015

Hello Shopper: [redacted]@gmail.com! To show you how much we truly value your years of business with us and to celebrate the continued success of our Prime membership program, we're rewarding you with-$100 in shopping points that can be used on any item on our online shopping site! (this includes any marketplace vendors)

In order to use this-$100 reward, simply go below to get your-coupon-card and then just use it during checkout on your next purchase. That's all there is to it!

Please visit-here now to get your reward

***DON'T WAIT! The Link Above Expires on 12/28!

→ Easy ways to protect yourself from phishing and malware cyber-attacks:

- Avoid websites that produce browser alerts and advise against access.
- Do not open email attachments or click links from unknown senders.
- Use a strong password and change it as required.

Smishing

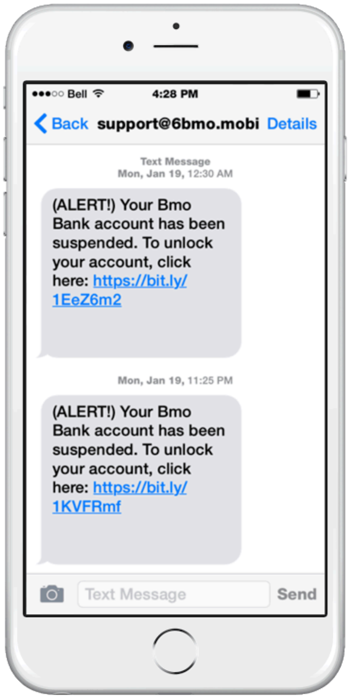
This cyber attack combines SMS (Short Message Service) with phishing. In this case, scammers send text messages pretending to be from reputable companies or authorities to trick you into revealing personal information, like passwords, credit card numbers, or other sensitive data, and click on links to reveal details about a false claim stated in the message.

Any text message with a warning about:

- Your account being compromised
- An unclaimed tax refund
- You missing a package delivery

*Or prompting you to click on a link, view an attachment or interact mindlessly with an unclear claim poses **red flags** you shouldn't ignore.*

Example of a Smishing attack



●●●○○ Bell 4:28 PM

Back support@6bmo.mobi Details

Text Message
Mon, Jan 19, 12:30 AM

(ALERT!) Your Bmo Bank account has been suspended. To unlock your account, click here: https://bit.ly/1EeZ6m2

Mon, Jan 19, 11:25 PM

(ALERT!) Your Bmo Bank account has been suspended. To unlock your account, click here: https://bit.ly/1KVFRmf

Text Message Send

Exercise caution when receiving suspicious text messages. Ask yourself if the organization would contact you this way, as most will not request personal or sensitive information via text.

- Avoid clicking on suspicious links or responding to suspicious texts.

- Instead of clicking on a link in a text message, you should manually type the web address into a browser.

- Fight the urge to click on a link because you fear missing out on something.

Steps to Protect Your Personal Information

Use Strong, Unique Passwords

- Create passwords that are hard to guess: mix uppercase and lowercase letters, numbers, and symbols.
- Don't use the same password for different accounts.
- Think about using a password manager to save and create secure passwords.

Enable Multi-Factor Authentication (MFA)

Requiring a second verification form, such as a code sent to your phone or app, adds extra security.

Be Careful with Personal Information

- Limit what you share: do not post sensitive details like your full name, address, or birthday on social media.
- Be cautious with requests: verify any unexpected requests for your personal details, whether online or by phone.

Monitor Your Accounts Regularly

- Check your bank and credit card statements often for unauthorized transactions.
- Review your credit reports each year to find errors or signs of fraud.

Secure Your Devices

- Use and regularly update antivirus software.
- Keep your operating system and apps updated to fix security issues.
- Turn on device encryption to protect your data on phones, laptops, and other devices.

Be Wary of Phishing Scams

Check the sender's identity before giving any personal information.

Protect Your Wi-Fi Network

Use a strong password for your home Wi-Fi.

Secure Your Online Accounts

Set up account recovery options like security questions or a backup email.

Be Careful With App Permissions

Only permit apps to access the functions that are essential for their operation.

Definitions

★ **Account recovery options** help you get back into your account if you forget your password or can't sign in. They make it easier to regain access quickly and securely. Standard recovery options include using an alternate email address or phone number, answering security questions, and using an authenticator app.

★ **App Permissions:** control what parts of your device an app can access. When you install an app, it may ask for permission to use features or access data. Common app permissions include location, camera, microphone, contacts, storage, SMS, and phone.

★ **Antivirus software** protects your devices from harmful programs. It detects, stops, and removes malware that can damage your computer, steal your information, or disrupt your work.

★ **Attachment:** is a file or document sent by email or message. It can include different types of files, such as documents (e.g., Word files, PDFs) or Images (e.g., JPEGs, PNGs).

★ **Browser:** is a software application that lets you access and view websites. Microsoft Edge, Google Chrome, and Apple Safari are common web browsers.

★ **Browser alerts** are pop-up messages that appear in your web browser to inform you about important events. Websites create these alerts for various reasons, such as to give warnings, ask for confirmation, or provide information.

★ **Cyber scams** are fraudulent schemes carried out online to deceive individuals or organizations into giving away personal information, money, or access to sensitive data.

★ **Cyber-attacks** are actions cybercriminals take to exploit cyber threats and achieve their malicious goals.

★ **Cybercrime** is a criminal activity done using computers and the Internet.

★ **Cybersecurity** refers to the methods and tools used to protect systems, networks, and data from cyber threats and attacks. Its main goal is to keep information safe and ensure that it remains confidential, accurate, and available when needed.

★ **Data Breach:** is an incident where sensitive, confidential, or protected information is accessed, disclosed, or stolen by an unauthorized party.

★ **Disinformation** is false or misleading information that someone creates and spreads on purpose to deceive people.

★ **Encryption:** is the process of converting data to an unrecognizable or "encrypted" form.

★ **Hacker:** a person who uses their knowledge of computers and networks to access data or systems without permission.

★ **HTML** stands for "Hypertext Markup Language." HTML is the language used to create web pages.

★ **Identity theft** occurs when someone obtains and uses another person's personal information without permission, such as their name, Social Security number, credit card information, or other identifying details.

★**Link,** also called a hyperlink, is an element in HTML that allows you to move to a different location when you click or tap on it. You can find links on almost every web page, and they make it easy to navigate between different pages.

★**Misinformation** is false or inaccurate information spread without the intention to deceive. It is different from disinformation, which is shared to mislead people on purpose. Misinformation can be spread unintentionally by people who believe it is true.

★**Operating system (OS)** is software that controls a computer's core functions. It communicates with the hardware and allows programs to run.

★**Password Manager:** It keeps all your passwords safe and can create strong, unique passwords for you. This way, you don't need to worry about making or remembering usernames and complex passwords on your own.

★**Pop-up message** is a small window that appears on the webpage you are visiting. It can appear when you click a link or button or open automatically when you enter a site. Common uses for pop-up messages include advertisements, notifications, forms, and alerts.

★**Privacy settings** are options you can adjust to control who can access your personal information, how your data is used, and what kind of information is shared. They help you manage your digital footprint and secure personal data across different platforms and devices.

★ **Search engine** helps you find information online, like a digital detective. When you type in a question, it looks through an extensive collection of web pages to show you the most relevant results. Popular search engines include Google, Bing, and Yahoo. They use complicated formulas to find matches based on your keywords, how relevant the information is, and how users engage with it.

★ **Software** is a general term for the programs and applications that run on a computer.

★ **Targeted attack** is a type of cyber attack that focuses on a specific organization, individual, or system. Unlike random attacks, targeted attacks are planned carefully to achieve a specific goal. They usually target high-value targets to achieve the desired outcome.

★ **Web address,** also known as a URL (Uniform Resource Locator), is the address used to access websites and web pages on the Internet.

★ **Webpages** are the files that make up the World Wide Web. An individual webpage is a text document written in HTML (hypertext markup language).

Resources Available

➔ https://cyberseniors.org/connected-learning/
For a simple overview of scams and how to deal with them to help you be safer online, you can visit https://att.digitallearn.org/courses/online-fraud-and-scams

➔ OnGuardOnline.gov
Operated by the Federal Trade Commission (FTC), this site provides tips and technical guidance on cybersecurity issues. It also provides a guide on what to do if you pay someone you think is a scammer or give a scammer your personal information or access to your computer or phone.

➔ StaySafeOnline.org
It offers resources on various cybersecurity issues, including information on adjusting privacy settings on several popular platforms.