


Cyber Security Guide

How to Prevent Phishing Attacks

Defending Credentials, Data, and Devices from Malice Intent

Contents

IT Security Dos & Don'ts	3
Important Tips to Prevent Phishing Attacks	4
Social Engineering	5
Types of Phishing Attacks	6-7
Understanding Phishing Attacks (BECs)	8
Business Email Compromise Timeline	9



IT Security Dos & Don'ts

Passwords	<ul style="list-style-type: none"> • DO NOT use easy to guess passwords, like your home address or pet's name. • DO NOT share employee passwords with others or write them down, keep them confidential. • DO NOT share client credentials via email. 	<ul style="list-style-type: none"> • DO use strong passwords. Minimum of 10 characters using uppercase, lowercase, numbers, and special characters. • DO use different passwords for different accounts so other accounts are not compromised.
Receiving External Emails	<ul style="list-style-type: none"> • DO NOT reply-to emails requesting change in Office 365 email logon credentials. • DO NOT click on any links requesting change in Office 365 email logon credentials. • DO NOT open any attachments from an unknown email address or untrusted source. • DO NOT send any sensitive or personal information via email, internally or to external partner. 	<ul style="list-style-type: none"> • DO pay attention to phishing scams and watch for signs of a trap. • DO contact your company's IT Department if you have any questions or suspect you have received fraudulent email.
Company Issued Devices	<ul style="list-style-type: none"> • DO NOT install unauthorized applications on your Decision Resources device. • DO NOT allow an unauthorized technician' to remote into your device. 	<ul style="list-style-type: none"> • DO lock your device when not in use, especially when travelling, to prevent unauthorized access. • DO use a Decision Resources provided ZeroTrust Secure Network when connecting to public Wi-Fi. Public wireless networks are insecure!





Important Tips to Prevent Phishing Attacks

What is a Phishing Scam?

Phishing is the attempt to trick victims into sharing sensitive information such as usernames, passwords, and credit card details for malicious reasons, by disguising themselves as trustworthy entities in electronic communications. These fraudulent attacks are designed to trick you into opening a file, clicking on a link, or taking some other action, usually to get access to cash.

Think Before You Click

Always be wary of emails, links and attachments from unknown or suspicious sources, especially anything asking you to update or verify account information. If in doubt, don't click! Keep in mind that cybercriminals can create email addresses and websites that look legitimate. Look up the company's phone number on your own (don't use the one a potential scammer is providing) and call the company to ask if the request is legitimate.

Don't Give Your Information to an Unsecured Site

If the URL of the website doesn't start with "https", or you cannot see a closed padlock icon next to the URL, do not enter any sensitive information or download files from that site. Sites without security certificates may not be intended for phishing scams, but it's better to be safe than sorry.

Don't Be Tempted by Pop-ups

Pop-ups aren't just irritating; they are often linked to malware as part of attempted phishing attacks. Most browsers now allow you to download and install free ad-blocker software that will automatically block most of the malicious pop-ups. If one does manage to evade the ad-blocker though, don't be tempted to click! Occasionally pop-ups will try and deceive you with where the "Close" button is, so always try and look for an "x" in one of the corners.

Protect Your Data

As a rule of thumb, unless you 100% trust the site you are on, you should not willingly give out company or client data, sensitive information, or intellectual property. Make sure, if you have to provide sensitive information, that you verify the website is genuine, that the company is real and that the site itself is secure. Always try to provide sensitive information over phone if possible. NEVER provide sensitive information over email!

Social Engineering

What is Social Engineering?

Social engineering is a common tactic used by cybercriminals. It is used to manipulate and deceive individuals into revealing confidential information or performing actions that compromise their security.

The goal of social engineering is to exploit the human tendency to trust, be helpful, or act on emotions. Attackers will use psychological tricks to gain a victim's confidence and make them act against their best interest. These methods include:

- **Creating a sense of urgency**
- **Fear**
- **Authority**
- **Using familiarity to gain confidence**

By relying on human rather than technical vulnerabilities, social engineering remains sophisticated and difficult to detect.



Social Engineering Steps

1. Information Gathering

Gather information about the organization and its employees (job titles, roles and responsibilities, etc...).

2. Build Rapport

Once a hacker identifies a target, the attacker will build a rapport and gain their trust by appearing credible and trustworthy.

3. Request Information or Action

The attacker will then make a request for information or action that benefits them. They will use psychological tricks to persuade the target to comply.

4. Success

Finally, the attacker uses the information or action to achieve their goals, software or the theft of sensitive information, such as stealing money or sensitive data.

Types of Phishing Attacks

Phishing attacks can be difficult to spot without training. It's important to note that these attacks are constantly evolving. Attackers are always looking for new ways to bypass security measures and trick victims. The most common attacks are mass market, sphere phishing, whaling, and clone phishing.

Mass Market Email Phishing

This is the most common type of phishing attack. Attackers will send fake emails designed to look like they come from a legitimate source. The goal is to trick users into clicking a link, downloading an attachment that contains malware, or entering sensitive information.

Email phishing typically starts with a mass email campaign. Attackers will send out thousands of emails to potential victims and could appear to be from a bank, e-commerce site, or social media business. They'll often include logos, graphics, and other elements that make them look convincing.

The email may contain a request to click on a link or download an attachment. They often present a sense of urgency, such as warning victims that an account is compromised, or a bill is overdue.

Spear Phishing

This is a more targeted form of phishing. Attackers will research their victims in advance and use personal information to create a highly compelling message. This means they'll comb social media profiles and research where the victim works and who they interact with. In doing so, they're able to build a complete profile of the victim. This background makes spear phishing more personalized, convincing, and harder to detect.

A spear-phishing email will often include a sense of urgency or importance. They want you to act quickly, without taking time to verify the email legitimacy.

The email may contain a request to click on a link or download an attachment. Like email phishing, this can result in the installation of malicious software or the theft of sensitive information.



Types of Phishing Attacks Cont.

Whaling

This attack targets high-level executives or other high-profile individuals in the business. Attackers are “hunting” for the “big fish”. Whaling attacks are personalized, sophisticated, and often rely on extensive research on their target. Like spear phishing, this can include research into social media, job titles, and relationships with colleagues and business partners.

The attacker can then carefully craft an email that appears to be from a trusted source. This might be a senior executive within the company, a business partner, or a government official.

The email may request sensitive information or access to sensitive accounts. These attacks rely on social engineering techniques to trick a target into taking action.

Whaling attacks can have serious consequences for businesses. Targeting high-profile workers mean that a successful attack can result in the theft of sensitive information, financial loss, and damage to the company's reputation.

Clone Phishing

With clone phishing, the attacker creates a nearly identical copy of a legitimate email or website. They'll then replace certain elements with malicious content.

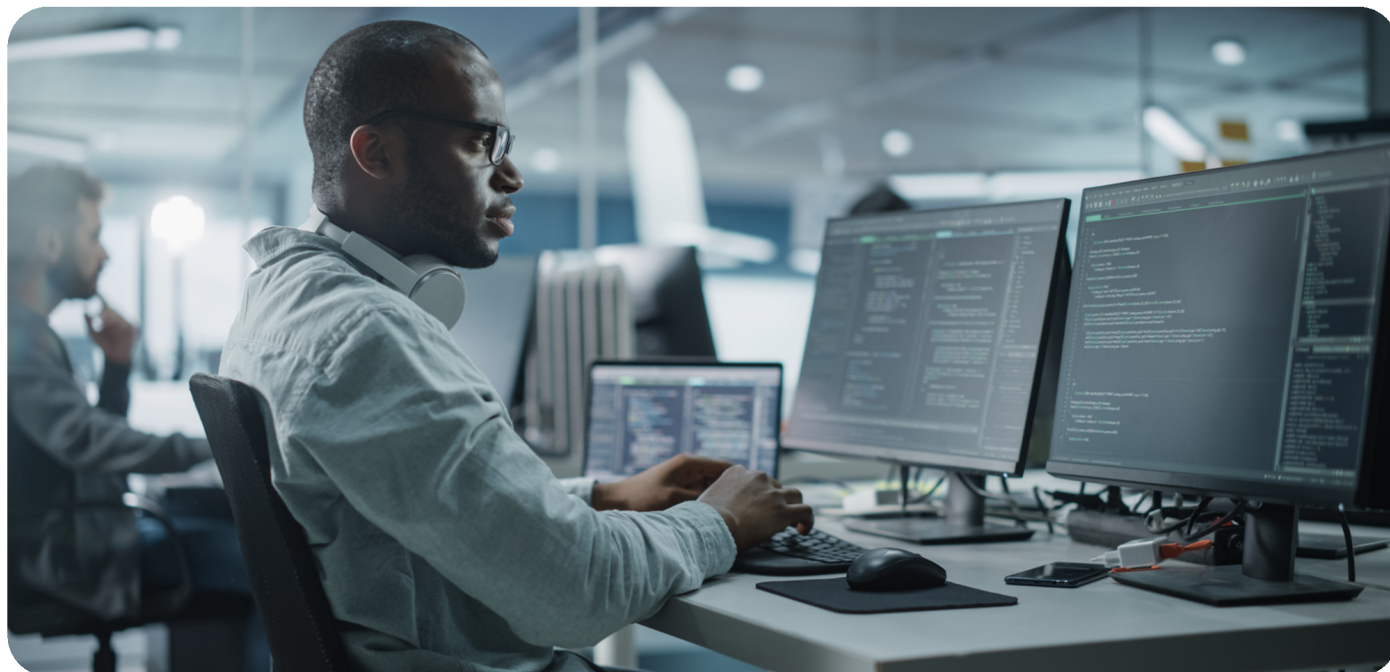
The goal is to trick the recipient into believing the email or website is legitimate. From there, they'll attempt to persuade the recipient to take action that may result in malicious behavior.

The clone will look almost identical, including logos, graphics, and other notable design elements. It may even come from a legitimate email or URL.

The attacker will typically make subtle changes to the clone email or webpage. For example, replacing a legitimate link with a harmful one, or requesting sensitive information where it otherwise wouldn't have.



Understanding Phishing Attacks (BECs)



Business Email Compromise

Business email compromise (BEC)—also known as email account compromise (EAC)—is one of the most financially damaging online crimes. It exploits the fact that so many of us rely on email to conduct business—both personal and professional. In a BEC scam, criminals send an email message that appears to come from a known source making a legitimate request, like:

- A vendor your company regularly deals with sends an invoice with an updated mailing address.
- A company CEO asks his assistant to purchase dozens of gift cards to send out as employee rewards. He asks for the serial numbers so she can email them out right away.
- A homebuyer receives a message from his title company with instructions on how to wire his down payment.

How Criminals Carry Out BEC Scams

- Spoof an email account or website. Slight variations on legitimate addresses like john.kelly@decision.com vs. john.kelley@decision.com can fool victims into thinking fake accounts are authentic.
- Send spear phishing emails that trick victims into revealing confidential information. That information lets criminals access company accounts, calendars, and data that gives them the details they need to carry out the BEC schemes.
- Use malware. Malicious software can infiltrate company networks and gain access to legitimate email threads about billing and invoices. That information is used to time requests or send messages, so accountants or financial officers don't question payment requests. Malware also lets criminals gain undetected access to a victim's data, including passwords and financial account information.

Business Email Compromise Timeline

An outline of how the business email compromise is executed by many organized crime groups.



Step 1: Identifying a Target

Organized crime groups target businesses in the U.S. and abroad by exporting information available online to develop a profile on the company and its executives.



Step 2: Grooming

Spearphishing emails and/or phone calls target a victim company's officials (typically in the financial department). Perpetrators use persuasion and pressure to manipulate and exploit employees' human nature. Grooming may occur over a few days or weeks.



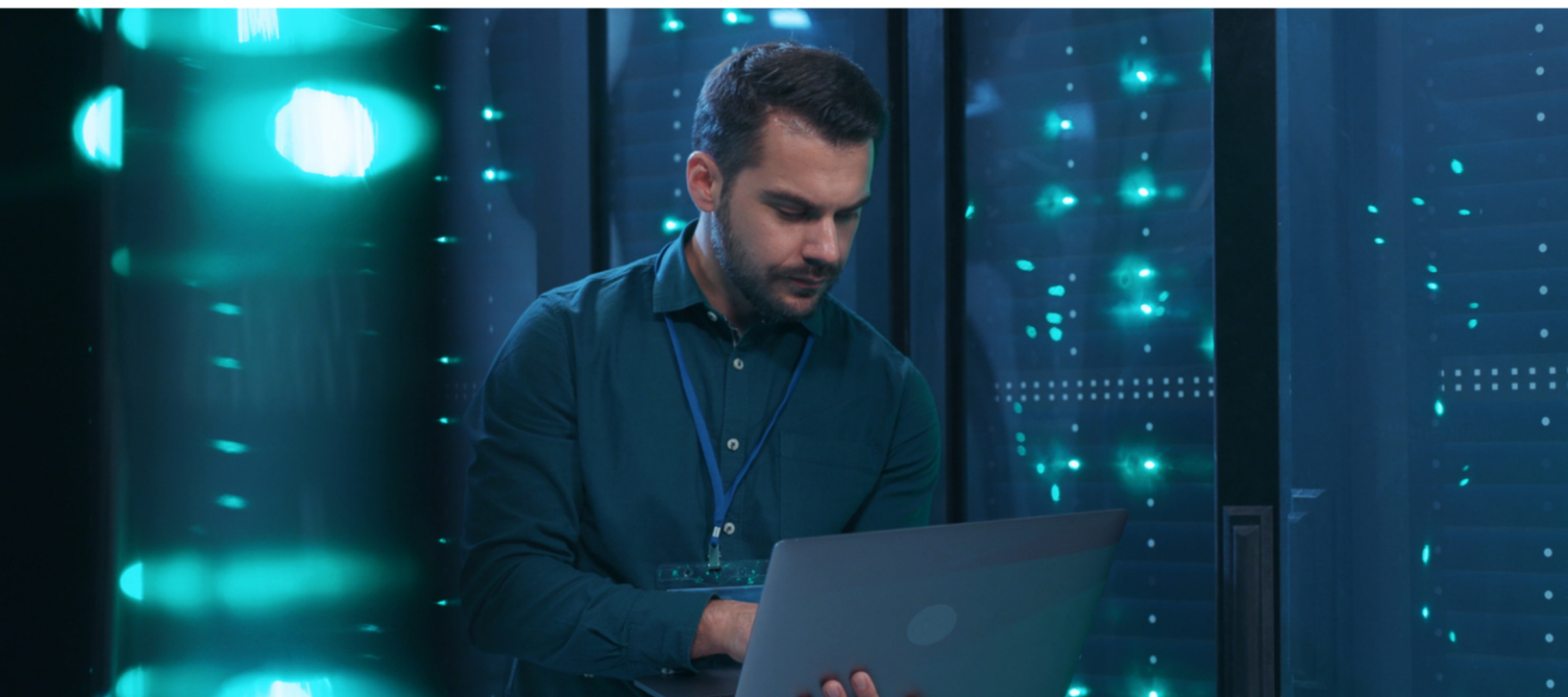
Step 3: Exchange of Information

The victim is convinced they are conducting a legitimate business transaction. The unwitting victim is then provided wiring instructions.



Step 4: Wire Transfer

Upon transfers, the funds are steered to a bank account control by the organized crime group. Perpetrators may continue to manipulate the victims into transferring more funds over time.





412.562.9660 | info@decision.com | decision.com