Don't Become a Victim!

Kevin Mitnick, "*The World's Most Wanted Hacker*" and KnowBe4's Chief Hacking Officer, gives you the information you need to protect yourself against the strategies and techniques hackers use to take control away from you and your organization.

DIGITAL ATTACKS

Phishing: Email-based social engineering targeting an organization.

Spear Phishing: Email-based social engineering targeting a specific person or role.

Stop, look, and think before you click that link or open that attachment.

IN-PERSON ATTACKS

USB Attacks: An attack that uses a thumb drive to install malware on your computer.

Tailgating: When a hacker bypasses physical access controls by following an authorized person inside.

Stop, look, and think before plugging any external media into your computer or allowing someone in that you don't recognize.

PHONE ATTACKS

Smishing: Text-based social engineering.

Vishing: Over-the-phone-based social engineering.

Stop, look, and think before you surrender confidential information or take action on an urgent request.

Social Engineering

Social engineering is the art of manipulating, influencing, or deceiving you into taking some action that isn't in your own best interest or in the best interest of your organization.

The goal of social engineers is to obtain your trust, then exploit that relationship to coax you into either divulging sensitive information about yourself or your organization or giving them access to your network.

Red Flags

Red flags are a sign of danger or a problem. They can be as subtle as an uneasy feeling or as obvious as an email about "suspicious charges" from a bank that you don't even have an account with.

Pay attention to these warning signs as they can alert you to a social engineering attack!

Since phishing is the most common form of social engineering, let's take a closer look at seven areas in an email and their corresponding red flags.

FROM

- An email coming from an unknown address.
- You know the sender (or the organization), but the email is unexpected or out of character.

TO

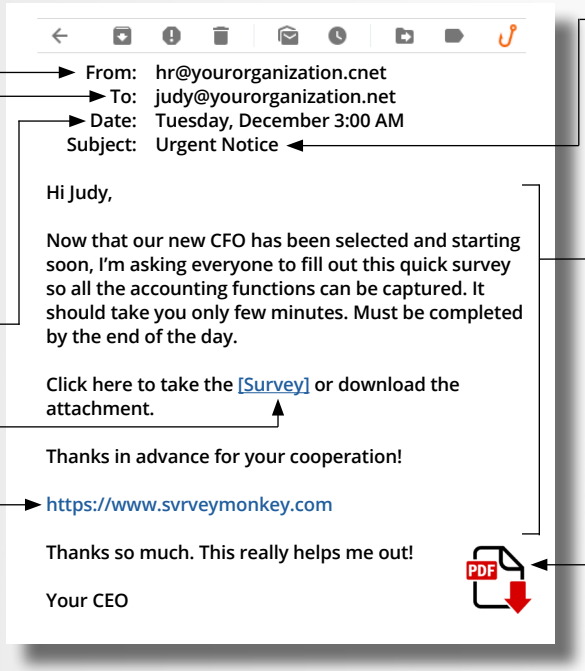
- You were copied on an email and you don't know the other people it was sent to.

DATE

- You receive an email that you would usually get during normal business hours, but it was sent at 3:00 a.m.

HYPERLINKS

- There are misspellings in the link.
- The email contains hyperlinks asking you to take an action.
- When you hover your cursor over the link, the link address is for a different website.



SUBJECT

- The subject line of an email is irrelevant or doesn't match the message content.
- It's an email about something you never requested or a receipt for something you never purchased.

CONTENT

- The sender is asking you to click on a link or open an attachment.
- The email is asking you to look at a compromising or embarrassing picture of yourself or someone you know.
- You have an uncomfortable feeling, or it just seems odd or illogical.

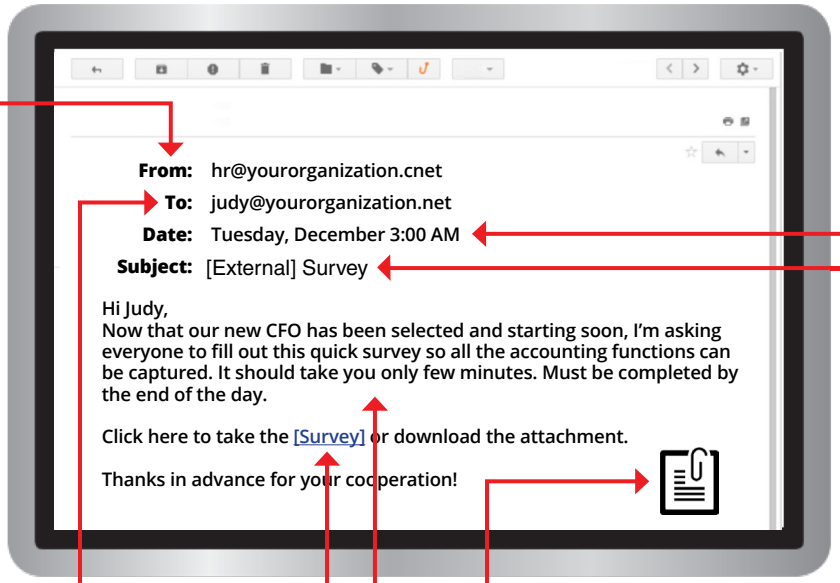
ATTACHMENTS

- Any attachment you receive that you aren't expecting.

Social Engineering Red Flags

FROM

- I don't recognize the sender's email address as someone **I ordinarily communicate with**.
- This email is from **someone outside my organization and it's not related to my job responsibilities**.
- This email was sent from **someone inside the organization** or from a customer, vendor, or partner and is **very unusual or out of character**.
- Is the sender's email address from a **suspicious domain** (like micorsoft-support.com)?
- **I don't know the sender personally** and they **were not vouched for** by someone I trust.
- **I don't have a business relationship** nor any past communications with the sender.
- This is an **unexpected or unusual email** with an **embedded hyperlink or an attachment** from someone I haven't communicated with recently.



DATE

- Did I receive an email that I normally would get during regular business hours, but it was **sent at an unusual time** like 3 a.m.?

SUBJECT

- Did I get an email with a subject line that is **irrelevant** or **does not match** the message content?
- Is the email message a reply to something **I never sent or requested**?
- **[External]** displayed in the subject line is a tool to help you identify emails from outside our organization that requires extra caution. Take time to slow down and check for red flags in the email.

TO

- I was cc'd on an email sent to one or more people, but **I don't personally know** the other people it was sent to.
- I received an email that was also sent to an **unusual mix of people**. For instance, it might be sent to a random group of people at my organization whose last names start with the same letter, or a whole list of unrelated addresses.

ATTACHMENTS

- The sender included an email attachment that **I was not expecting** or that **makes no sense** in relation to the email message. (This sender doesn't ordinarily send me this type of attachment.)
- I see an attachment with a possibly **dangerous file type**.

HYPERLINKS

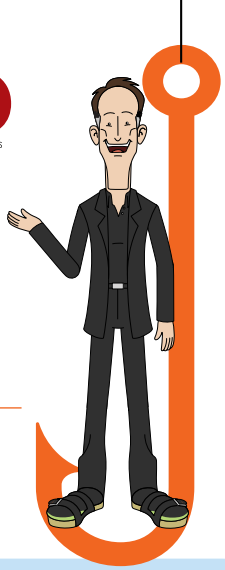
- I hover my mouse over a hyperlink that's displayed in the email message, but the **link-to address is for a different website**. (This is a **big** red flag.)
- I received an email that only has **long hyperlinks with no further information**, and the rest of the email is completely blank.
- I received an email with a **hyperlink that is a misspelling** of a known website. For instance, www.bankofarnerica.com — the "m" is really two characters — "r" and "n."

CONTENT

- Is the sender asking me to click on a link or open an attachment to **avoid a negative consequence** or to **gain something of value**?
- Is the email **out of the ordinary**, or does it have **bad grammar** or **spelling errors**?
- Is the sender asking me to click a link or open up an attachment that **seems odd** or **illogical**?
- Do I have an **uncomfortable gut feeling** about the sender's request to open an attachment or click a link?
- Is the email asking me to look at a **compromising or embarrassing picture** of myself or someone I know?

BE A HERO!

Use the Phish Alert Button



You receive an email asking you to take an action. Sounds suspicious, right? But don't worry. You can be a hero by taking the correct action–and giving your IT department the information they need to defend your organization against the effects of malicious email attacks. It's easy. Thanks to the **Phish Alert Button**, or **PAB** for short.

How do I know what to report?

You should only report messages you suspect are malicious, like **phishing** or **spear phishing** emails. Reporting annoying messages, like **spam**, to IT will waste their time and resources.

Spam is unsolicited and unwanted email, typically sent to try to sell you something. While it is often annoying and misleading, it is rarely malicious.

Simply delete it!

Phishing messages are bulk emails, typically appearing to be from a reputable source, that ask you to take a specific action that can cause damage to you or your organization. These messages are malicious.

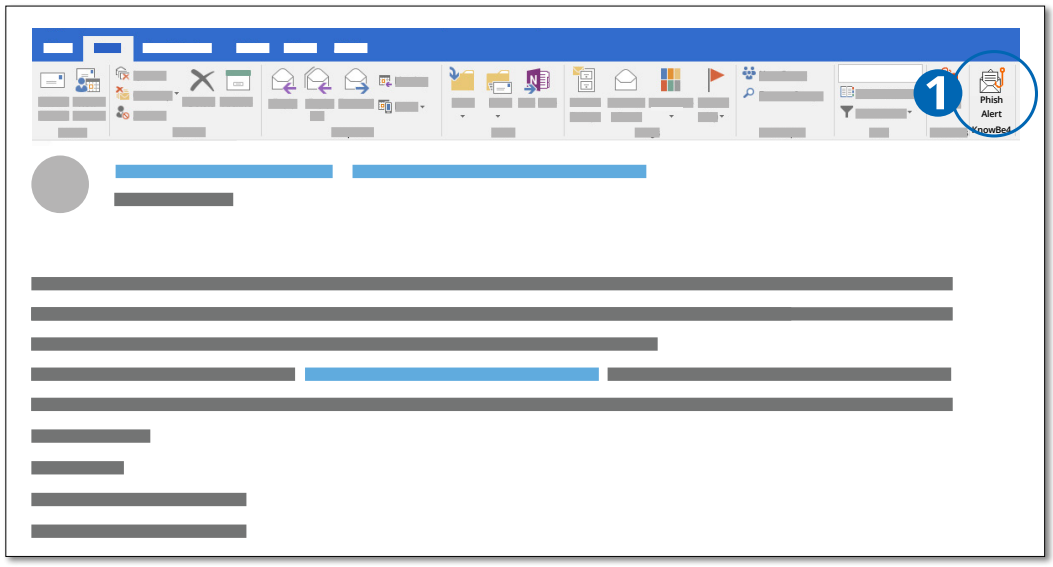
Spear phishing emails are targeted attacks on a person or organization, occurring after detailed research in order to make them seem especially real. These messages are extremely malicious and can lead to very damaging consequences.

Report it with the PAB!

Where do I find the PAB in Outlook?

While viewing your email:

❶ You can find the Phish Alert Button in the Outlook ribbon at the top of your screen. Locate the envelope icon with the orange "fish hook."

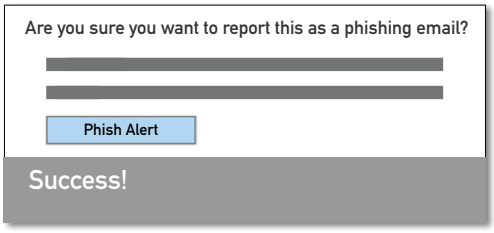


Report:

Report suspected phishing emails by clicking the Phish Alert in the ribbon.

Confirm:

Once you click to report, the pop-up will prompt you to confirm your action. Once confirmed, the suspicious email will be immediately forwarded to your IT team.



Stop. Look. Think. Report!

Remember, you are the last line of defense against email based criminal activity. Never click on a link or open an attachment in any unexpected or unsolicited email. If you are uncertain, follow your organization's security policy–or ask your IT team for advice.

KnowBe4
Human error. Conquered.

COMPUTER, EMAIL AND INTERNET USAGE POLICY

Objective
Team Allied Distribution recognizes that use of the internet and email is necessary in the workplace, and employees are required to use both responsibly and lawfully, as unacceptable use can place Team Allied Distribution and others at risk for harassment, security breaches and similar issues. This policy outlines the guidelines for acceptable use of Team Allied Distribution's technology systems.

Scope
This policy must be followed in conjunction with other Team Allied Distribution policies governing appropriate workplace conduct and behavior. Any employee who abuses the company-provided access to email, the internet, or other electronic communications or networks, including social media, may be denied future access and, if appropriate, be subject to disciplinary action up to and including termination. Team Allied Distribution complies with all applicable federal, state and local laws as they concern the employer/employee relationship, and nothing contained herein should be misconstrued to violate any of the rights or responsibilities contained in such laws.

Questions regarding the appropriate use of Team Allied Distribution's electronic communications equipment or systems, including email and the internet, should be directed to your supervisor or the information technology (IT) department.

Policy
Team Allied Distribution has established the following guidelines for employee use of the company's technology and communications networks, including the internet and email, in an appropriate, ethical and professional manner.

Confidentiality and Monitoring
All technology provided by Team Allied Distribution, including computer systems, communication networks, company-related work records and other information stored electronically, is the property of Team Allied Distribution and not the employee. In general, use of the company's technology systems and electronic communications should be job-related and not for personal convenience. Team Allied Distribution reserves the right to examine, monitor and regulate email and other electronic communications, directories, files and all other content, including internet use, transmitted by or stored in its technology systems, whether onsite or offsite.

Internal and external email, voice mail, text messages and other electronic communications are considered business records and may be subject to discovery in the event of litigation. Employees must be aware of this possibility when communicating electronically within and outside the company.

Appropriate Use
Team Allied Distribution employees are expected to use technology responsibly, lawfully and productively as necessary for their jobs. Internet access and email use is for job-related activities only.

Employees may NOT use Team Allied Distribution's internet, email or other electronic communications to transmit, retrieve or store any communications or other content of a defamatory, discriminatory, harassing or pornographic nature. No messages with derogatory or inflammatory remarks about an individual's race, age, sex, disability, religion, national origin, physical attributes, gender identity, sexual preference or any other protected class may be transmitted. Harassment of any kind is prohibited.

Abusive, excessively profane or offensive language and any illegal activities—including piracy, cracking, extortion, blackmail, copyright infringement and unauthorized access to any computers on the internet or email—are forbidden.

Copyrighted materials belonging to entities other than Team Allied Distribution may not be transmitted by employees on the company's network without permission of the copyright holder.

Employees may not use Team Allied Distribution's computer systems in a way that disrupts its use by others. This includes sending or receiving excessive numbers of large files and spamming (sending unsolicited email to thousands of users).

Employees are prohibited from downloading software or other program files or online services from the internet without prior approval from the IT department. All files or software should be passed through virus-protection programs prior to use. Failure to detect viruses could result in corruption or damage to files or unauthorized entry into company systems and networks.

Every employee of Team Allied Distribution is responsible for the content of all text, audio, video or image files that he or she places or sends over the company's internet and email systems. No email or other electronic communications may be sent that hide the identity of the sender or represent the sender as someone else. Team Allied Distribution's corporate identity is attached to all outgoing email communications, which should reflect corporate values and appropriate workplace language and conduct.

Nothing in this policy is intended to, nor should be construed to limit or interfere with employee rights as set forth under all applicable provisions of the National Labor Relations Act, including Section 7 and 8(a)(1) rights to organize and engage in protected, concerted activities regarding the terms and conditions of employment.