OCTOBER 26, 2022 / / WEDNESDAY / / ISSUE 8

SECURITY NEWS

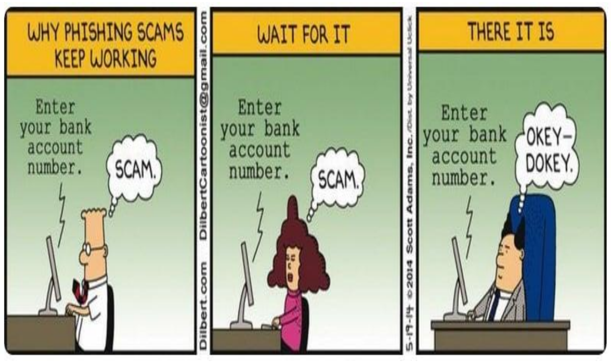
CYBERSECURITY AWARENESS

It's Fall Y'all

CHRIS MCDANIEL
OCTOBER 2022

As we all prepare for this crazy fall weather of hot and cold the Yadkin County IT Department has some warm news to share with you. As we move closer to the end of October and start getting ready for the holiday season. We would like to remind everyone to stay cyber aware and ahead of the cybercriminals by protecting your information. As we continue moving forward to better protect the county and its staff, IT has started implementing Cisco DUO within the county. This is a platform used for two factor authentication which will have you verify who you are when logging into the county systems and applications. We have also started new hire orientation training to help our new employees learn all the great benefits and resources we have to offer. Another great opportunity that is in the planning stages is we will be offering IT training for all county employees on the new Microsoft O365 platform as well as all the great resources it has to offer.

Just a friendly reminder if you have not completed your KnowBe4 Security Awareness Training please do so as soon as possible as this will help teach you better ways to protect yourself from cyber threats. Lastly, remember the attackers are out there constantly looking for new ways to steal our information. Let's not fall prey to their tricks and work hard to keep them away. Remember to Think Before You Click. Hope Everyone has a Great Day and Stays Safe.


WHY PHISHING SCAMS KEEP WORKING
Enter your bank account number.
SCAM.
WAIT FOR IT
Enter your bank account number.
SCAM.
THERE IT IS
Enter your bank account number.
OKEY-DOKEY.
Dilbert.com DilbertCartoonist@gmail.com
© 2014 Scott Adams, Inc.

MFA Fatigue Attack

NCDIT
SEPTEMBER 2022

Multifactor authentication (MFA) is a good way to protect end user accounts from cyberattackers trying to gain access to them. A cost-effective part of the Zero Trust model, MFA offers another form (or factor) of protection, along with passwords, in the authentication process to verify the actual identity of the user trying to access an account.

Although it improves access control to any given system, attackers have found ways to compromise MFA via social engineering. One such way is "MFA Fatigue." MFA Fatigue should not be confused with "password fatigue," in which a person is overburdened with the number of passwords or PINs they must remember for multiple accounts or events. MFA Fatigue is not overly sophisticated, but it has become extremely effective because it targets the human factor via social engineering.

What is MFA Fatigue?

MFA Fatigue is a technique that enemies use to flood a user's authentication app with push notifications. The intent is to attract the victim to accept an MFA prompt and therefore enable an attacker to gain entry to an account or device.

For this kind of attack to work, the attacker must already possess the victim's credentials, which could be obtained through brute forcing (i.e., guessing username and passwords to gain unauthorized access) or password reuse (i.e., the user having the same password across different accounts or services). With the victim's credentials, the attacker repeatedly sends valid push notifications to the victim (normally through a mobile app). Eventually, the victim tires of the flood of MFA notifications and responds to them. If the victim "approves" the MFA notification, the attacker gains access to the victim's account or device.

Success from an MFA Fatigue attack usually occurs because the user is distracted or overwhelmed by the notifications. In some cases, it can be misinterpreted as a bug or confused with other legitimate authentication requests.

One recent incident involved a Cisco employee's credentials being compromised after an attacker gained control of an account through an MFA Fatigue attack. GoSecure, a cybersecurity company that provides endpoint, network and email threat detection, published a proof of concept that shows how the attack works.

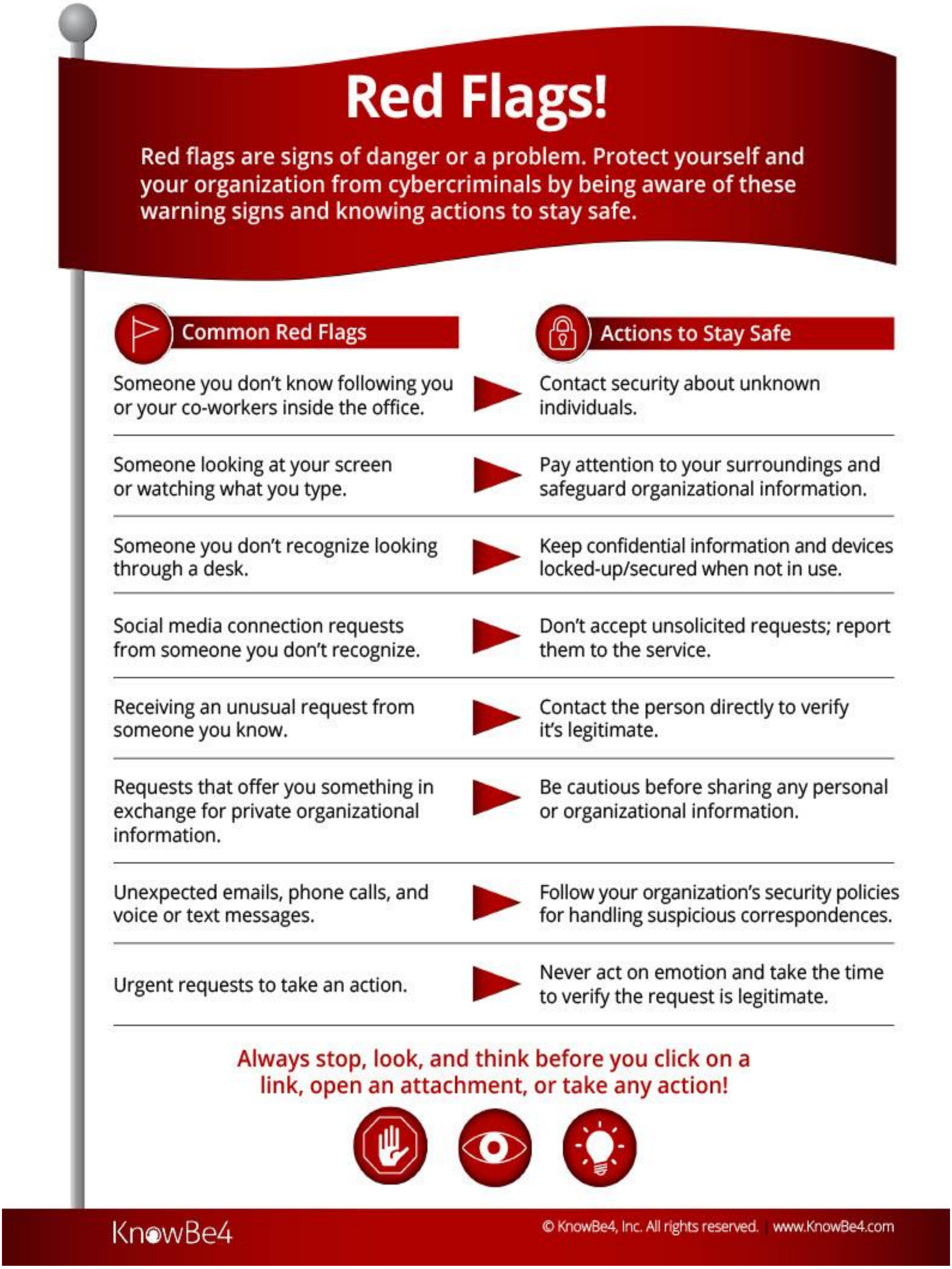
How can MFA Fatigue be prevented?

The following are ways to reduce the risk of someone becoming a victim to MFA Fatigue.

1. Since the attack begins with a password compromise, users should use unique and complex passwords for each of their accounts, and not reuse passwords for multiple accounts. They should change passwords frequently and avoid sharing them with others. For more information, review the state of NC's password management policy.
2. Do not accept MFA service prompts if you have not recently logged in to a service that uses MFA service. If it looks suspicious or unexpected, do not approve the MFA prompt. Report the incident using your organization's incident response procedures.
3. Identity and access management (IAM) administrators can also do the following:
    - Set default limits of the MFA service to lower the number of push notifications allowed in a certain timeframe.
    - Implement a second sign-in mechanism called "number matching."
    - Enable conditional access or some other verification when access is requested from a previously unknown source/device.

According to one leading identify and access management company, the best approach to solving MFA Fatigue may be a combination of prevention (implementing MFA), detection (alerting and responding to threats), and user awareness.

This article provided by NCDIT and may be found via the link provided here: NCDIT.



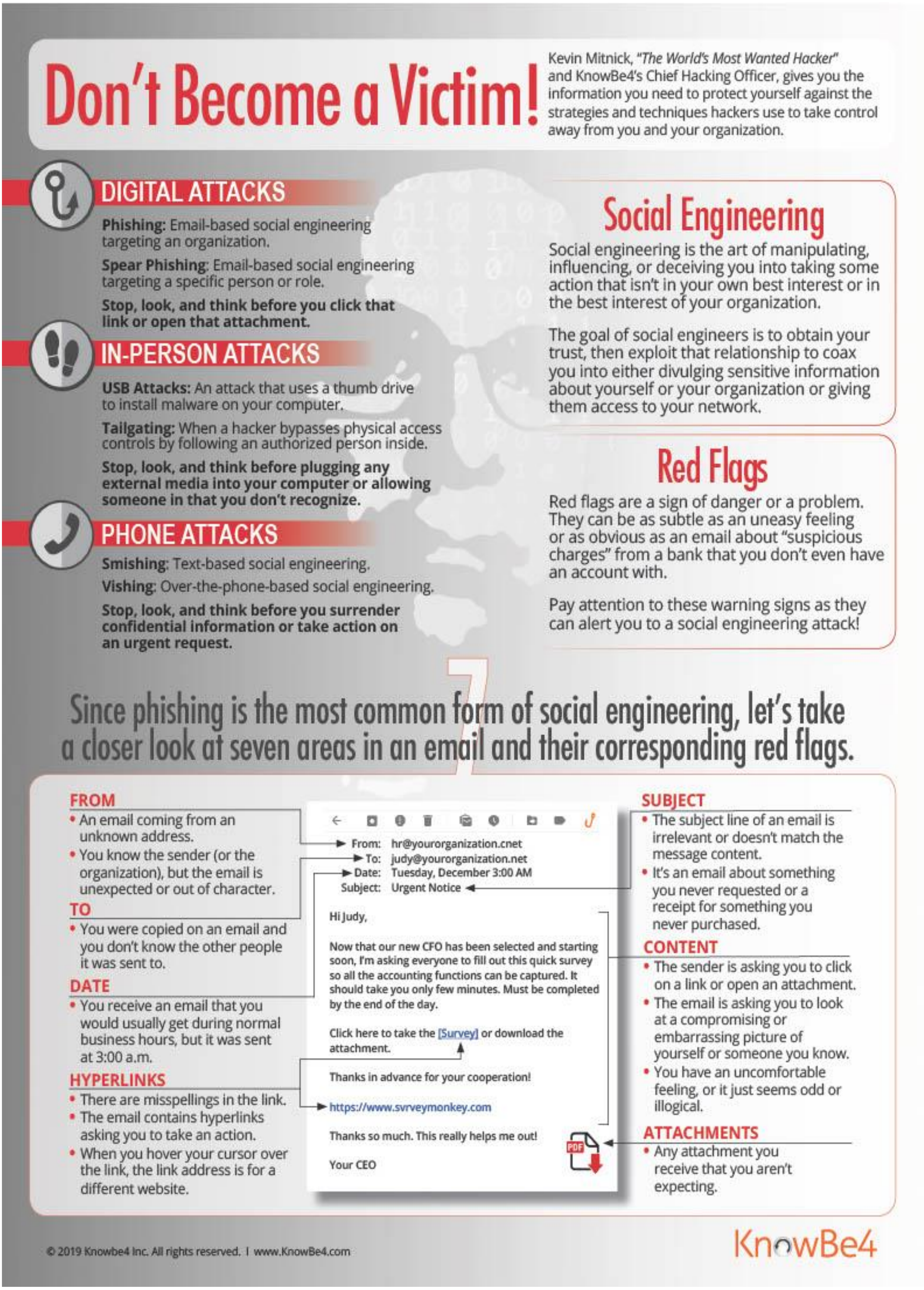
Red Flags!

Red flags are signs of danger or a problem. Protect yourself and your organization from cybercriminals by being aware of these warning signs and knowing actions to stay safe.

Common Red Flags		Actions to Stay Safe
Someone you don't know following you or your co-workers inside the office.	▶	Contact security about unknown individuals.
Someone looking at your screen or watching what you type.	▶	Pay attention to your surroundings and safeguard organizational information.
Someone you don't recognize looking through a desk.	▶	Keep confidential information and devices locked-up/secured when not in use.
Social media connection requests from someone you don't recognize.	▶	Don't accept unsolicited requests; report them to the service.
Receiving an unusual request from someone you know.	▶	Contact the person directly to verify it's legitimate.
Requests that offer you something in exchange for private organizational information.	▶	Be cautious before sharing any personal or organizational information.
Unexpected emails, phone calls, and voice or text messages.	▶	Follow your organization's security policies for handling suspicious correspondences.
Urgent requests to take an action.	▶	Never act on emotion and take the time to verify the request is legitimate.

Always stop, look, and think before you click on a link, open an attachment, or take any action!

KnowBe4



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.

From: hr@yourorganization.cnet
To: judy@yourorganization.net
Date: Tuesday, December 3:00 AM
Subject: Urgent Notice

Hi Judy,

Now that our new CFO has been selected and starting soon, I'm asking everyone to fill out this quick survey so all the accounting functions can be captured. It should take you only few minutes. Must be completed by the end of the day.

Click here to take the [Survey] or download the attachment.

Thanks in advance for your cooperation!

https://www.svrveymonkey.com

Thanks so much. This really helps me out!

Your CEO

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.

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!

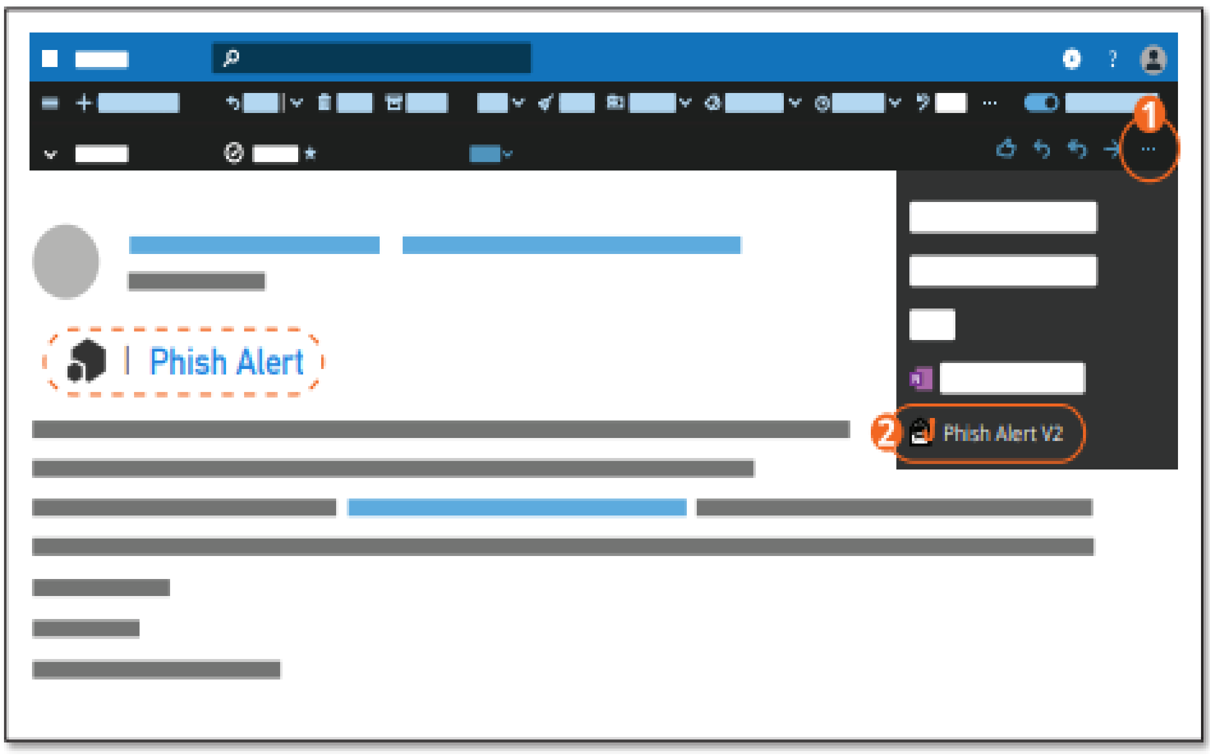
Where do I find the PAB in the new Outlook for Office 365?

While viewing your email:

❶ You can find the Phish Alert Button by clicking the ellipses (or three dots) in the right side to open a menu. ❷ You can then click the Phish Alert Button at the bottom of the menu.

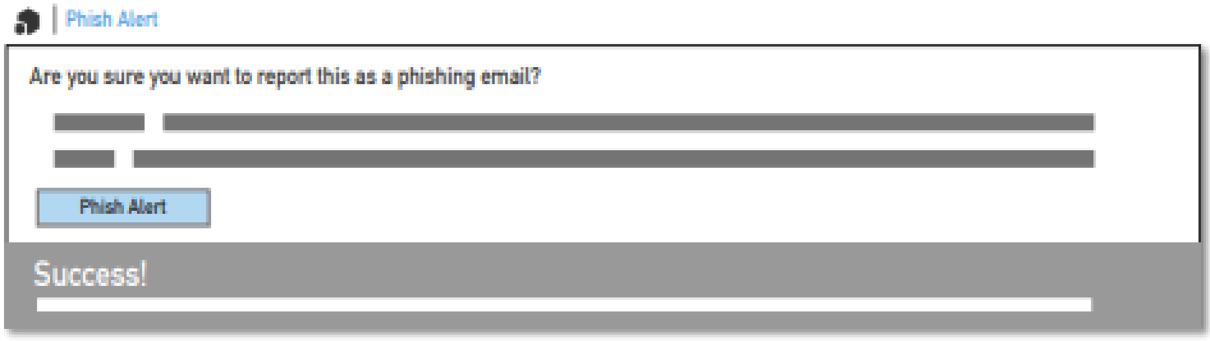
— or —

You can also click the words "Phish Alert" in the text link toward the top of an open email.



Confirm:

The pop-up box you see will prompt you to confirm your action. Once confirmed, the email in question will be immediately forwarded to your organization's IT team.



Are you sure you want to report this as a phishing email?

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.