OCTOBER 5, 2023 / / THURSDAY / / ISSUE 9

SECURITY NEWS

CYBERSECURITY AWARENESS

PUMPKIN SPICE LATTES, HALLOWEEN, AND
NATIONAL CYBERSECURITY AWARENESS MONTH

I.T. NEWS

CHRIS MCDANIEL
OCTOBER 2023

As we all prepare for this hot and cold soon to be fall weather the Yadkin County IT Department would like to remind everyone to stay cyber aware and ahead of cybercriminals by protecting your information online. October is Cybersecurity Awareness Month, where many places share the importance of cybersecurity. This is the perfect opportunity to take advantage of educational sessions and training to help you learn best practices and tools that can enhance your security methods. As we continue moving forward to better protect the county and its staff, IT is still in the process of implementing Cisco DUO throughout the county. This is a platform used for multifactor authentication which will have you verify who you are when logging into the county systems and applications. Another great opportunity that is still in the planning stages is IT will be offering training for all county employees on the new Microsoft O365 platform as well as all the great resources it has to offer. We would also like to get your thoughts and ideas on some training classes you would like to see offered, please reach out to Chris McDaniel by email and let him know. 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 that attackers are out there constantly looking for new ways to steal your 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.

'Secure Our World:' October is Cybersecurity Awareness Month

NCDIT
OCTOBER 2023

October brings in the annual occurrence of Cybersecurity Awareness Month, a time where the public and corporate sectors, as well as tribal communities, spread awareness of the value of cybersecurity. This annual initiative was set in place to promote the importance of good online security practices and the need for appropriate cyber defense mechanisms.

This year's theme is **'Secure Our World'** and focuses on four simple ways to help you stay safe online:

1. **Recognize and report phishing.** Avoid clicking links or opening attachments in suspicious messages. If there is any doubt, check with the sender first.
2. **Use strong passwords and a password manager.** All passwords should be long, complex, and unique. Never reuse passwords; use password managers to generate and store strong passwords.
3. **Turn on multifactor authentication.** It requires you to enter additional information such as a text code or fingerprint rather than just your password.
4. **Update software.** Make sure your devices are running the latest version of operating systems, software, and web browsers.

Throughout October, various organizations, educational institutions, and businesses will host events, workshops, and training programs to help educate people on varying cyberthreats, data protection methods, and different ways to safeguard personal information online.

Not only is security an individual effort, but it is also a collective effort as well. During Cybersecurity Awareness Month, take the time to evaluate the different methods you and your organization use to secure your devices and online presence. Take time to learn about cybersecurity threats, best practices, and tools you can use to enhance your security.

Finally, remember, you are the first line of defense in true security. Please stay cyber aware and vigilant and always think before you click.

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

Online Security for Kids

Diana Kelley, SANS, September 6, 2023

Background

Our kids' lives are online today more than ever, from socializing with friends and gaming, to online learning and education. Ask yourself this question, how can we help our kids make the most of online technology, safely and securely?

Education and Communication

First and foremost, make sure that you are fostering good open communications with your children. Far too often, parents get caught up in the technology required to block content or determining which mobile apps are good or bad. Ultimately, keeping our kids safe is less about technology and more about behavior and values. A great place to start is by creating a list of expectations with your kids. Here are some factors to consider (Note that these rules should evolve as kids get older.):

- Decide on times when they can or cannot go online for fun, and for how long. For example, you may want to be sure children complete all their homework or chores before gaming online or social networking with friends and limit the amount of time they are allowed online each day.
- Identify the types of websites, mobile apps, and games that they can access online and why they are appropriate or not.
- Determine what information they can share and with whom. Children often do not realize that what they post online is public, permanent, and accessible to anyone. In addition, anything they share privately with their friends can (and often is) shared with others without them knowing.
- Identify who they should be reporting problems to, for example, strange pop-ups, scary websites, or if someone online is being a bully or creepy. It's critical that children feel safe talking to a trusted adult.
- Just like in the real world, teach children to treat others online as they would want to be treated themselves, with respect and dignity.
- Ensure children understand that people online may not be who they claim to be, and that not all information is accurate or truthful.
- Define what can be purchased online and by whom, including in-game purchases.

Over time, the better they behave and the more trust they gain, the more flexibility you may want to give them. Once you decide on the rules, post them in the house. Even better, have your kids contribute to the rules and sign the document so that everyone is in full agreement.

The earlier you start talking to your kids about your expectations, the better. Not sure how to start the conversation? Ask them which apps they are using and how they work. Put your child in the role of teacher and have them show you what they are doing online. Consider giving them some "What if…" scenarios to reinforce the positive digital behaviors you've discussed or agreed upon. Keeping communication open and active is the best way to help kids stay safe in today's digital world.

For mobile devices, consider a central charging area somewhere in your house. Before your children go to bed, have set times when all mobile devices are placed in the charging area so your children are not tempted to use them when they should be sleeping.

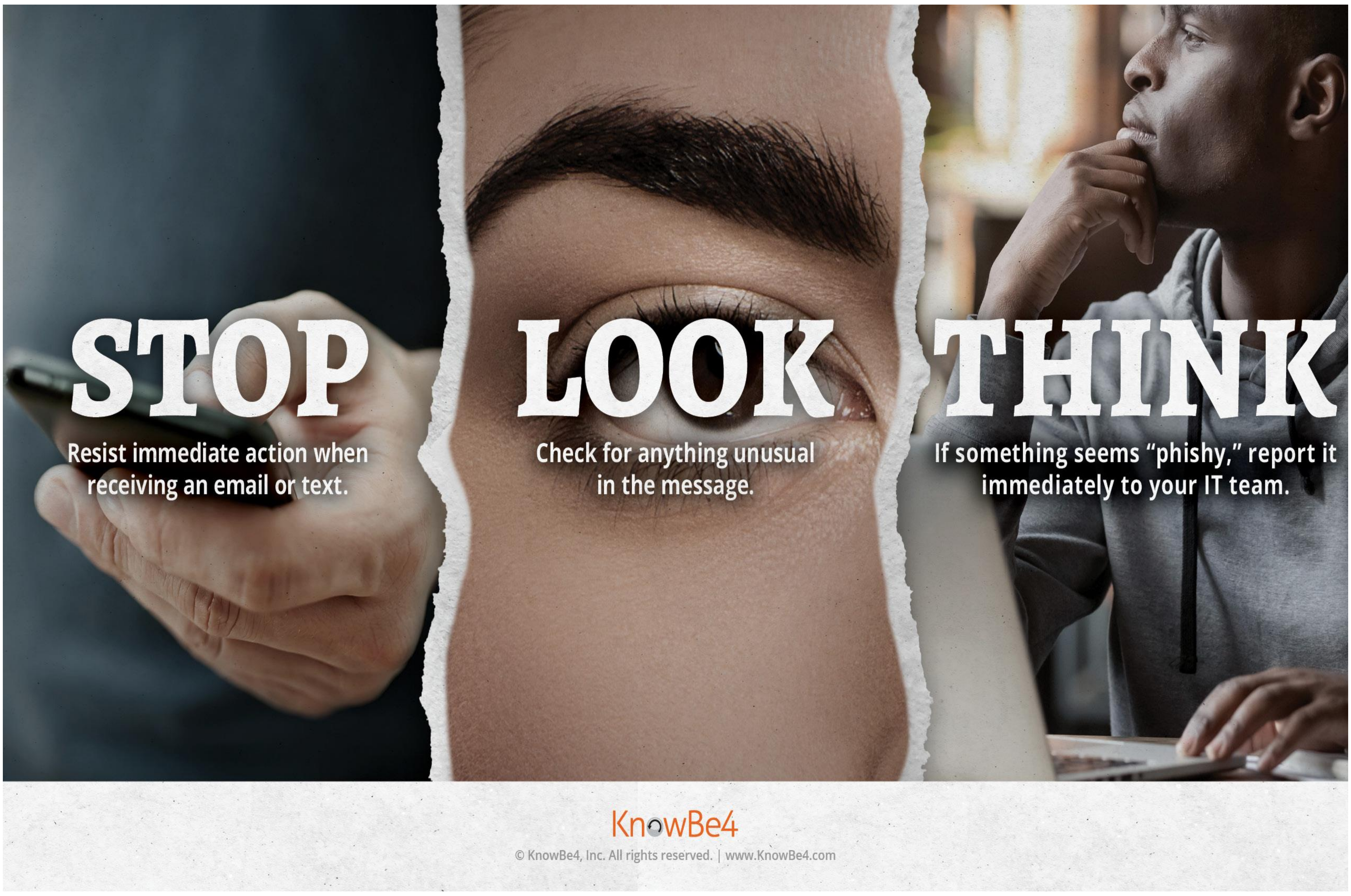
Security Technologies and Parental Controls

There are security technologies and parental controls you can use to monitor and help enforce the rules. These solutions tend to work best for younger children. Older kids don't only need more access to the internet but often use devices that you may not control or can't monitor, such as school-issued devices, gaming consoles, or devices at a friend's or relative's house. In addition, older children can often circumvent purely technological attempts to control them. This is why, ultimately, communication, values, and trust with children are so important.

Leading by Example

Remember to set a good example as parents or guardians. When your kids talk to you, put your own digital device down and give them your full attention. Consider not using your digital devices at the dinner table, and never text while you're driving. Finally, when your kids make mistakes, treat each one as an experience to learn from instead of simply punishing them. Make sure they feel safe approaching you when they experience anything uncomfortable, or they realize that they have made a mistake online.

The information for this article from SANS may be found via the link provided here: SANS OUCH! Newsletter.


STOP
Resist immediate action when receiving an email or text.
LOOK
Check for anything unusual in the message.
THINK
If something seems "phishy," report it immediately to your IT team.
KnowBe4
© KnowBe4, Inc. All rights reserved. | www.KnowBe4.com

YOUR PASSWORD STRENGTH

Cybercriminals love weak passwords! **Protect yourself and your organization** with these best practices:

- **Don't share** your password.
- **Change** your password regularly.
- Make passwords **hard to guess**.
- **Use a different** password for each app and website.

KnowBe4

WHY SECURITY AWARENESS TRAINING?
RANSOMWARE
PHISHING
CEO FRAUD
COMPLIANCE
THAT'S WHY
KnowBe4
Human error. Conquered.

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!

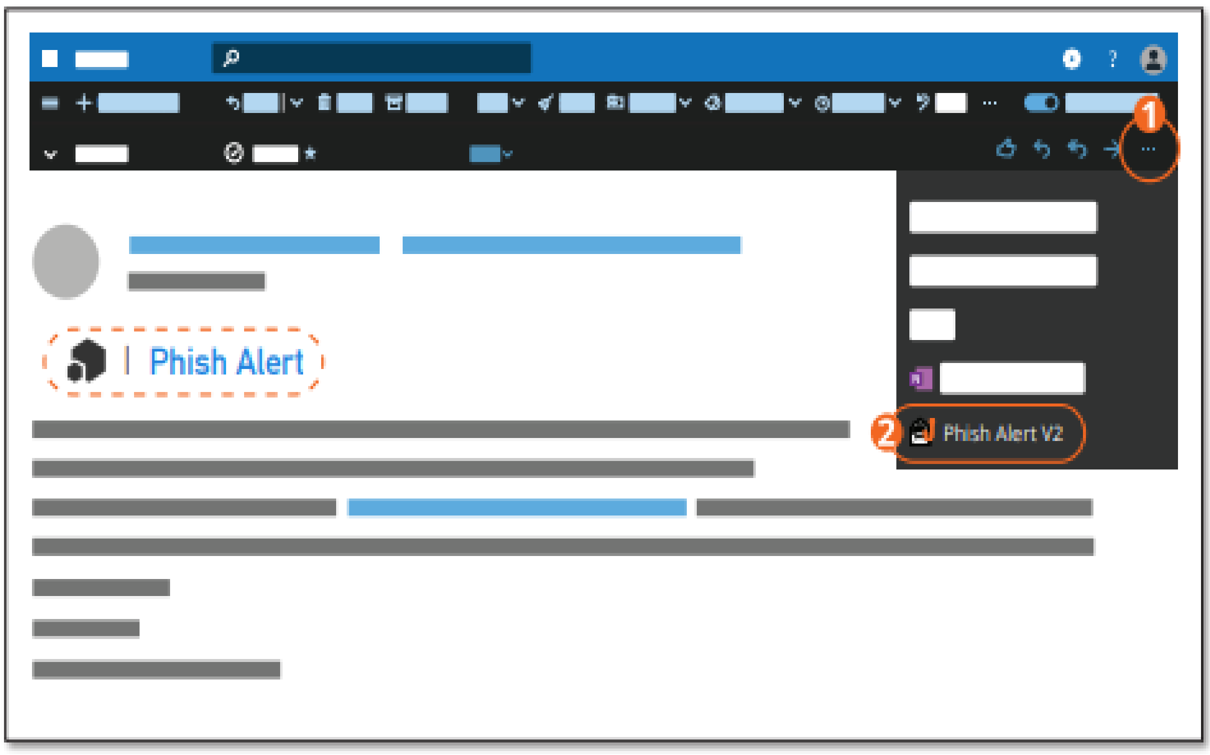
Where do I find the PAB in the new Outlook for Office 365?

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.

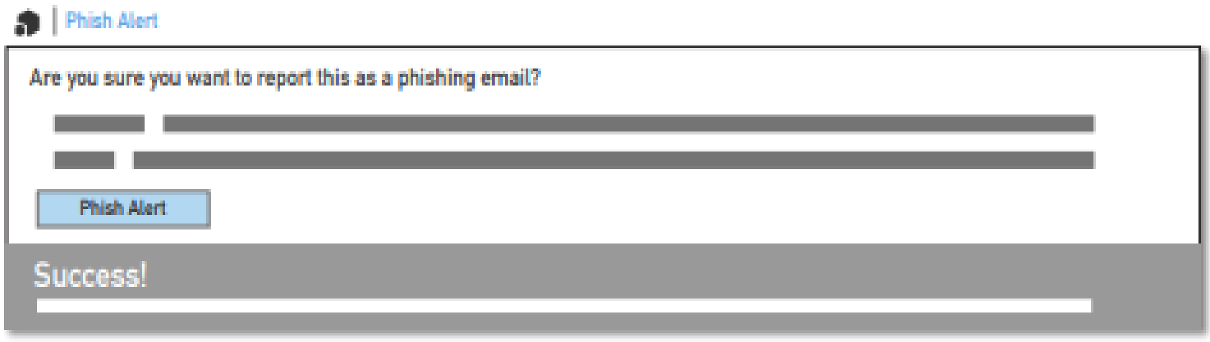
or

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?

Phish Alert

Success!

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.