JUNE 23, 2022 / / THURSDAY / / ISSUE 7

SECURITY NEWS

SOCIAL MEDIA SAFETY

Things are Heating Up

CHRIS MCDANIEL
JUNE 2022

As we all prepare for the hot and scorching weather the Yadkin County IT Department has some hot news to share with you. As most of you know we have officially implemented everyone to the new email system, and everyone should have their email back. If you don't, please let us know by submitting an IT request ticket and we can get that corrected for you. Also, we would like to share more exciting things that are coming to better assist you with your work and the recent changes that were made. We are looking forward and getting prepared to start offering training classes for everyone that would like to learn how to use and implement all the great features we have and can do with the new system. We are also looking to start holding an IT version of new hire orientation to show the new employees all the great resources they will have the opportunity to use.

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.

Cybercriminal Steals 1 Million Facebook Account Credentials Over 4 Months

TECHREPUBLIC
JUNE 9, 2022

As phishing attacks continue to be a go-to for threat actors, one scam found that a user had stolen a million Facebook account credentials over the span of four months. Anti-phishing company PIXM found that a fake login portal was being used for Facebook as a stand-in for the social media site's landing page, and users were entering their account information in an attempt to log in to the site only to have their information stolen.

"It's impressive the amount of revenue that a threat actor can generate even without resorting to ransomware or other common forms of fraud like requesting gift cards or emergency PayPal requests," said Chris Clements, vice president of solutions architecture at cybersecurity company Cerberus Sentinel. "With enough scale, even actions like advertising referrals that result in pennies can add up to amounts that become compelling for cybercriminals to exploit."

Phishing Tactics Used to Steal Facebook Credentials

When PIXM dug further into the fake landing page, they found "a reference to the actual server which hosted the database server to collect users' entered credentials", which had been modified from that of the legitimate URL, and led to a series of redirects. Also within the code, PIXM discovered a link to a traffic monitoring application, which allowed the anti-phishing company to view the tracking metrics. This led to PIXM to uncover not only the traffic information from the cybercriminals page, but also a host of other fake landing pages as well.

"People often underestimate the value of their social media accounts, failing to enable MFA and otherwise protect their accounts from cybercriminals. Unfortunately, when bad actors take over an account, it is often used to attack their own friends and family," said Erich Kron, security awareness advocate at KnowBe4. "Through the use of a real account that has been compromised, bad actors will use the trust inherent in a known connection to trick people into taking actions or risks they normally would not."

The links found were to be originating from Facebook itself, as threat actors would gain access to a victim's account, then send harmful links in mass to the victim's friends to cultivate more account credentials. Using services like glitch.me, famous.co, amaze.co and funnel-preview.com, the websites would deploy and generate URLs of the fake Facebook page, thus tricking individuals into entering and having their account information stolen. After further investigation the attacks appeared to be coming from a threat actor in Colombia, along with the email address of the person performing the attacks.

Ways to Avoid Falling Victim to Facebook Phishing

A major way to stop these attacks is by not clicking on links that seem phony or illegitimate, even if they seem to be coming from a friend or trusted source. Even though someone close to you may send you a link, doesn't mean it is actually coming from that person's account.

You should be aware of the type of fraud campaigns that cybercriminals are conducting and stay on guard. If you receive any unusual request from social media contacts make sure to verify, if possible, by calling them to make sure the request was legitimate.

The best way to avoid having your account compromised is by using MFA, which requires a code or string of numbers to be entered before someone can access your account. This can help deter cybercriminals by not having all the information needed to log into a compromised account.

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

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!

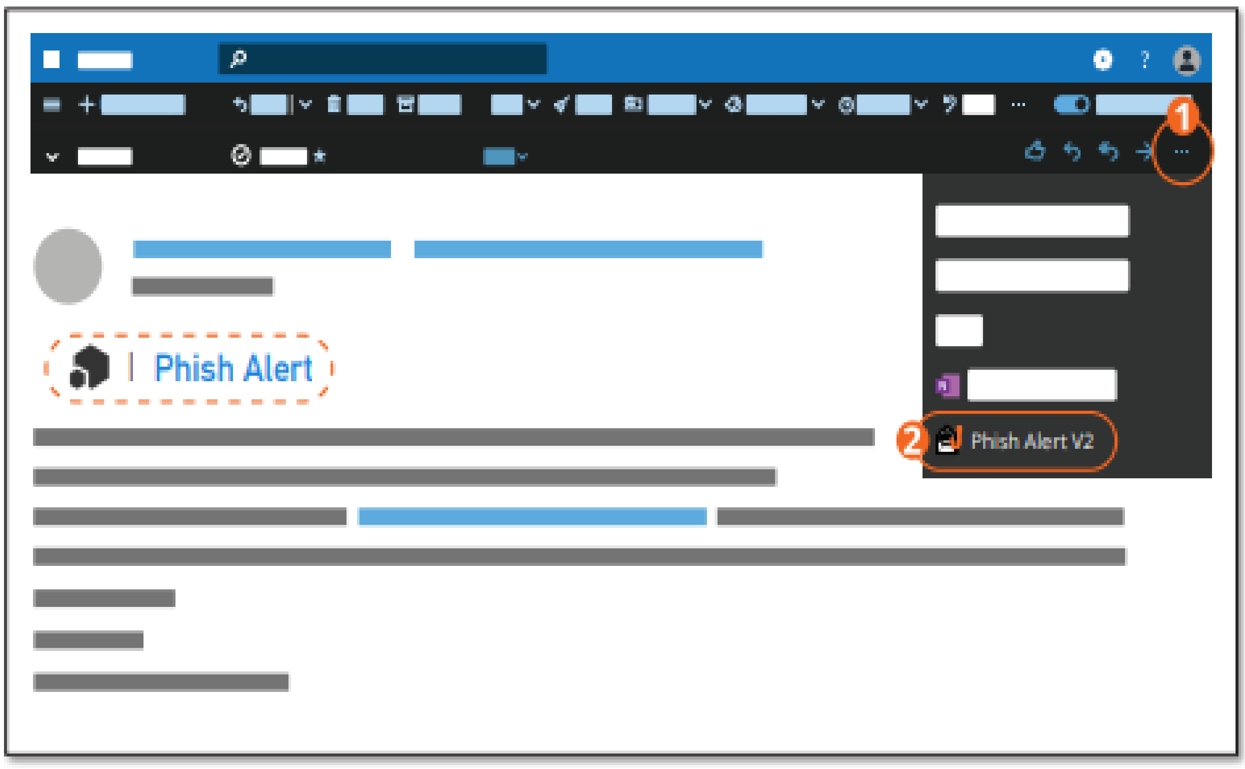
Where do I find the PAB in the new Outlook for Office 365?

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.

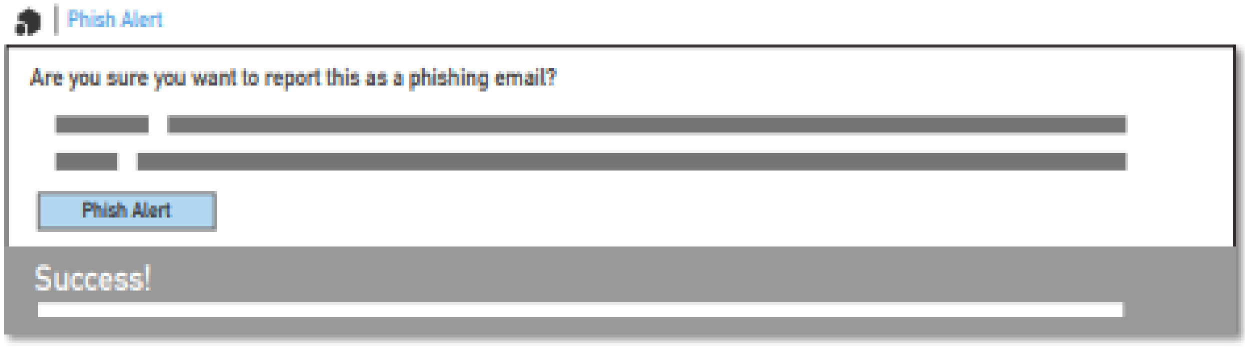
or

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.



Phish Alert

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

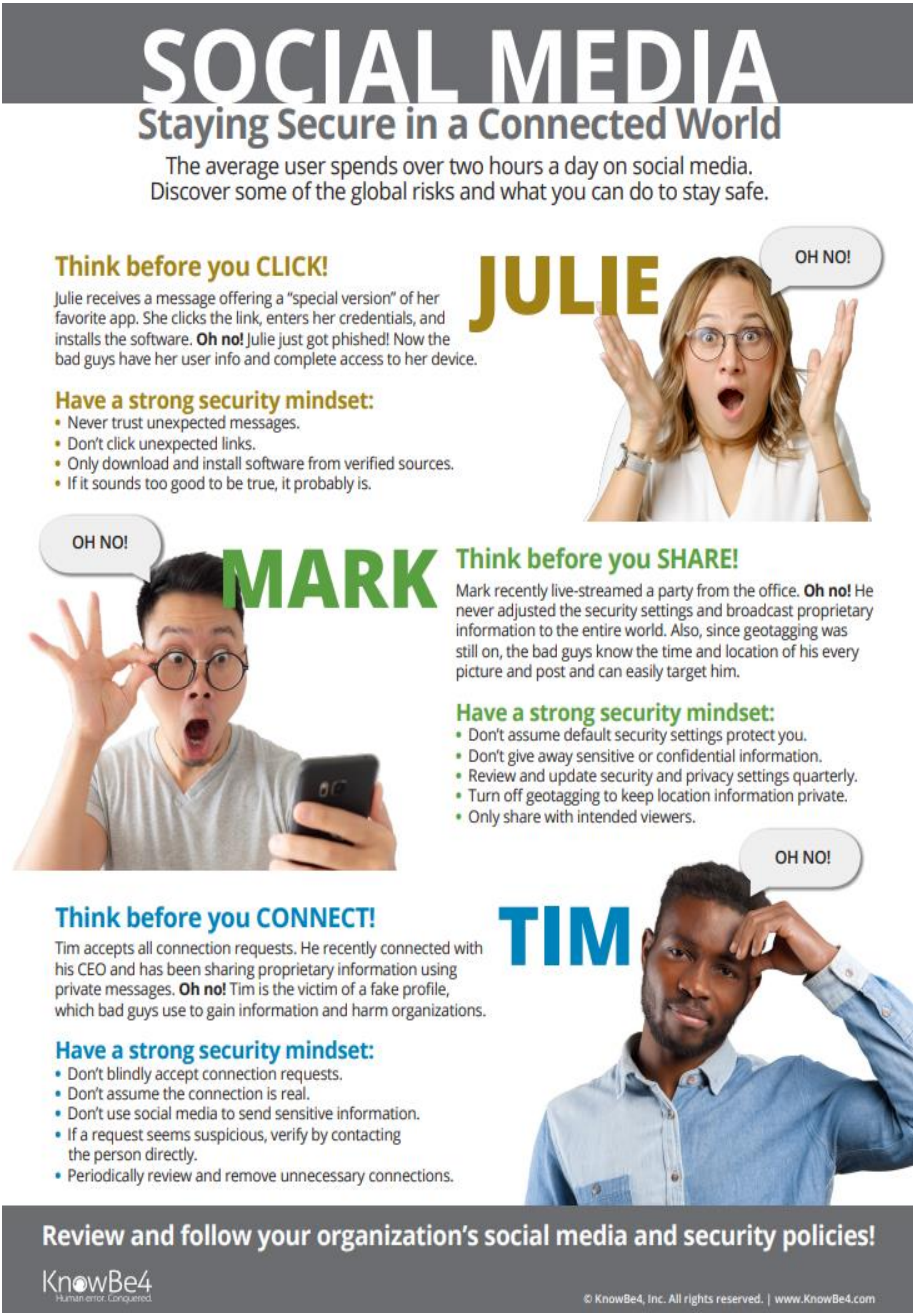
Phish Alert

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.



SOCIAL MEDIA

Staying Secure in a Connected World

The average user spends over two hours a day on social media. Discover some of the global risks and what you can do to stay safe.

JULIE

OH NO!

Think before you CLICK!

Julie receives a message offering a "special version" of her favorite app. She clicks the link, enters her credentials, and installs the software. **Oh no!** Julie just got phished! Now the bad guys have her user info and complete access to her device.

Have a strong security mindset:

- Never trust unexpected messages.
- Don't click unexpected links.
- Only download and install software from verified sources.
- If it sounds too good to be true, it probably is.

MARK

OH NO!

Think before you SHARE!

Mark recently live-streamed a party from the office. **Oh no!** He never adjusted the security settings and broadcast proprietary information to the entire world. Also, since geotagging was still on, the bad guys know the time and location of his every picture and post and can easily target him.

Have a strong security mindset:

- Don't assume default security settings protect you.
- Don't give away sensitive or confidential information.
- Review and update security and privacy settings quarterly.
- Turn off geotagging to keep location information private.
- Only share with intended viewers.

TIM

OH NO!

Think before you CONNECT!

Tim accepts all connection requests. He recently connected with his CEO and has been sharing proprietary information using private messages. **Oh no!** Tim is the victim of a fake profile, which bad guys use to gain information and harm organizations.

Have a strong security mindset:

- Don't blindly accept connection requests.
- Don't assume the connection is real.
- Don't use social media to send sensitive information.
- If a request seems suspicious, verify by contacting the person directly.
- Periodically review and remove unnecessary connections.

Review and follow your organization's social media and security policies!

KnowBe4
Human error. Conquered.

Don't Make Yourself a TARGET!

Be careful what you post on social media.

Don't share proprietary information about your organization.

Don't use social media to send sensitive information.

Don't assume default security settings protect you.

Hackers use the information you post to target you and your organization.

KnowBe4