FIGHTING SOCIAL MEDIA PHISHING ATTACKS: 10 TIPS

By Scott Matteson

TechRepublic

INTRODUCTION

Phishing, the practice of trying to lure unsuspecting victims to click on links to install malware or to divulge confidential information, is a tactic that involves more than just malicious emails. Phishing attacks can also take place in other environments, such as via texts, phone calls, or social media.

Facebook, in particular, seems especially prone to these types of nuisances, like those involving fake websites set up by scammers in the hopes of tricking people into revealing their account information. Facebook does offer some tips on combatting these efforts (such as being on the lookout for sloppy messages, messages that claim to have attached passwords, malicious links, or requests for confidential information). The threats also involve fake charity requests for victims of the latest natural disaster.

How can you avoid phishing? Below are tips from email security organization Proofpoint for both consumers and IT departments, which I combined with commentary based on my own experiences.

TIPS FOR CONSUMERS

1. Be wary of fake news

Social media con artists use divisive political content to enrage voters and spread misinformation. Avoid "fake news" or news of dubious accuracy and refrain from clicking on links sent to you or posted on social media. Think like a newsroom: You need to confirm accuracy. If you see a news story, verify it on an online news site. Never blindly repost information without checking for accuracy, no matter how much you might wish it to be true.

2. Be wary of bots

Keep an eye out for bot accounts and block them, since they aren't likely to promote honest or legitimate content. Be cautious of any Twitter and Facebook accounts where something doesn't look quite right, or they seem especially aggressive. Telltale signs of a bot include accounts with random names/numbers, accounts that frequently repost items, accounts posting material that doesn't seem relevant to the context of a discussion or thread, and accounts that contribute no actual content but just share/retweet other accounts.

3. Investigate details behind questionable ads

Use Facebook's "Info and Ads" to determine the motivations behind ads. For instance, when you see a political ad on Facebook that seems suspect or sensational, click the ad and then click the page associated with it. Facebook's goal is provide "increased accountability for bad actors, which will help to prevent abuse on Facebook" and to "bring additional transparency to Pages and the ads they're running."

If the ad comes from a less-than-reputable source, disregard future content from this page or entity, as phishing attempts are more likely from these types of accounts.

4. Avoid clicking links

Do not click on Twitter Direct Message (DM) or Facebook Messenger links unless you are positive they are reputable. They might contain malware or direct you to credential phishing sites that will attempt to steal your passwords or financial information or install malware on your system or device.

Links can also be obfuscated by adding a bunch of unnecessary words or random characters to what seems like a legitimate site in the hopes that you'll be fooled into opening them. For instance, a link to www.americanex-pressfinancialserviceadvice.com or www.citibank2018BBB.com might seem OK at first glance but look closer. You can highlight the link and press Ctrl+C to copy it, then open a text editor like Notepad and press Ctrl+V to paste it in for closer inspection.

5. Use a quality filter

If it is not already on, activate your quality Twitter filter. This tool (which is enabled by default) helps you locate the quality tweets amongst the noise generated by bots and other low-value entities.

To check your settings, click your profile picture at the top right of the Twitter site and then choose Settings. At the Settings screen, select Notifications from the left column. Check the Quality Filter box to enable the filter.

Note: Twitter says this "does not filter notifications from people you follow or accounts you've recently interacted with."

Also, verify that Twitter accounts purportedly owned by famous people or governmental officials really are who they say they are by ensuring there is a blue circle with a check in it next to their name or Twitter handle.

Finally, unfollow pages of dubious accuracy or pages prone to promoting sensationalistic "click bait" ads or posts.

TIPS FOR IT DEPARTMENTS

6. Know the current situation and share details

Monitor social media and make sure that individuals who are responsible for company social media posts or updates are aware of what to look for regarding common or new scams. Send weekly email updates or

broadcasts as needed to help educate personnel (but don't send too much communication or it may go unheeded).

Staff should also be wary of statements made on social media with no source material provided.

For example, if someone posts a quote attributed to a politician or business representative but doesn't provide a verifiable link to the source or other information to substantiate the details, don't trust it.

7. Establish official guidelines and restrictions

Review and update your digital and social media risk management strategy and governance, including policies, processes, and programs to specifically address the growing number and types of threats on social platforms. Include instructions about how to secure both branded and employee accounts.

Tech Pro Research offers various comprehensive policies covering technological topics. Its social media policy, as well as its identity theft protection policy, provide useful guidelines to help safeguard organizations.

8. Safeguard social media access

Mandate that social media postings, updates, or interactions be conducted only on approved devices (either company or employee-owned). Ensure that these devices contain the latest anti-malware software and controls, that they are set to lock either with strong passwords or biometric mechanisms, and that they can be remotely erased if lost or stolen.

9. Look at the big picture

Think comprehensively. As the number and types of risks continue to expand, the responsibility for managing digital and social media risks extends well beyond the IT department. Make sure you partner effectively across your organization. For instance, if social media is handled by outside agencies, make sure they follow security and policy guidelines and are aware of the latest developments.

10. Engage in minimalism

Limit social media sprawl: Account sprawl can run rampant and lead to fake and unmanaged accounts that can damage brand reputation and customer experience. Also, limit the number of people who have access to social media accounts—and change any passwords if they depart the organization.

CREDITS

Senior Director, B2B Editorial
Jason Hiner

Editor in Chief, UK
Steve Ranger

Senior Managing Editor
Bill Detwiler

Associate Managing Editor
Mary Weilage

Editor, Australia
Chris Duckett

Senior Editor
Alison DeNisco Rayome

Senior Features Editor
Jody Gilbert

Senior Writer
Teena Maddox

Chief Reporter
Nick Heath

Staff Writer
Macy Bayern

Associate Editor
Melanie Wachsman

Multimedia Producer
Derek Poore

Cover image:
iStock/Chainarong Prasertthai

TechRepublic

ABOUT TECHREPUBLIC

TechRepublic is a digital publication and online community that empowers the people of business and technology. It provides analysis, tips, best practices, and case studies aimed at helping leaders make better decisions about technology.

DISCLAIMER

The information contained herein has been obtained from sources believed to be reliable. CBS Interactive Inc. disclaims all warranties as to the accuracy, completeness, or adequacy of such information. CBS Interactive Inc. shall have no liability for errors, omissions, or inadequacies in the information contained herein or for the interpretations thereof. The reader assumes sole responsibility for the selection of these materials to achieve its intended results. The opinions expressed herein are subject to change without notice.