This publication is a public service of the Ohio Department of Education, the Ohio Cyber Range Institute, and the University of Dayton Center for Cybersecurity and Data Intelligence.

Becoming CYBERMINDFUL

For you. For everyone.

IN THIS ISSUE:

DON'T GET HOOKED BY SOCIAL ENGINEERING

Phishing is such a constant threat, we're devoting an entire issue of **Becoming Cybermindful** to recognizing some common warning signs.

Warning!

If you see any of these in your email messages, don't take the bait. These warning signs don't *guarantee* the email's a phish, but they're things to consider before opening attachments, clicking links, or complying with unexpected requests or demands.

PRO TIP:
You can't "hover" over a link from your mobile device, but you can "press-and-hold" to pop up the link-to address instead!

Warning: Attachments!

- The sender included an attachment you were not expecting or that makes no sense in relation to the email message.
- This sender doesn't ordinarily send you these types of attachments.
- You see an attachment with a possibly dangerous file type (like ".exe").

Warning: Hyperlinks!

- When you hover your mouse over a hyperlink in the email message, the "link-to" address points to a different website (a big red flag!).
- The email has long hyperlinks and no further information or text.
- The hyperlink is a misspelling of a known web site. For instance, bankofarnerica.com (the "m" is really two characters – "r" & "n").

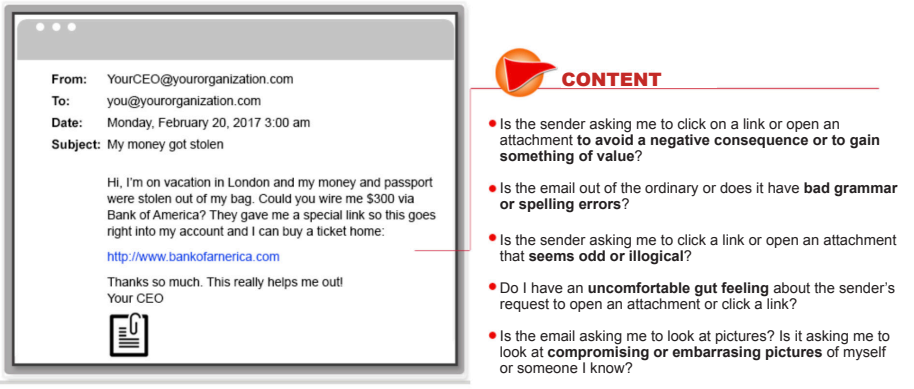
Warning: Content!

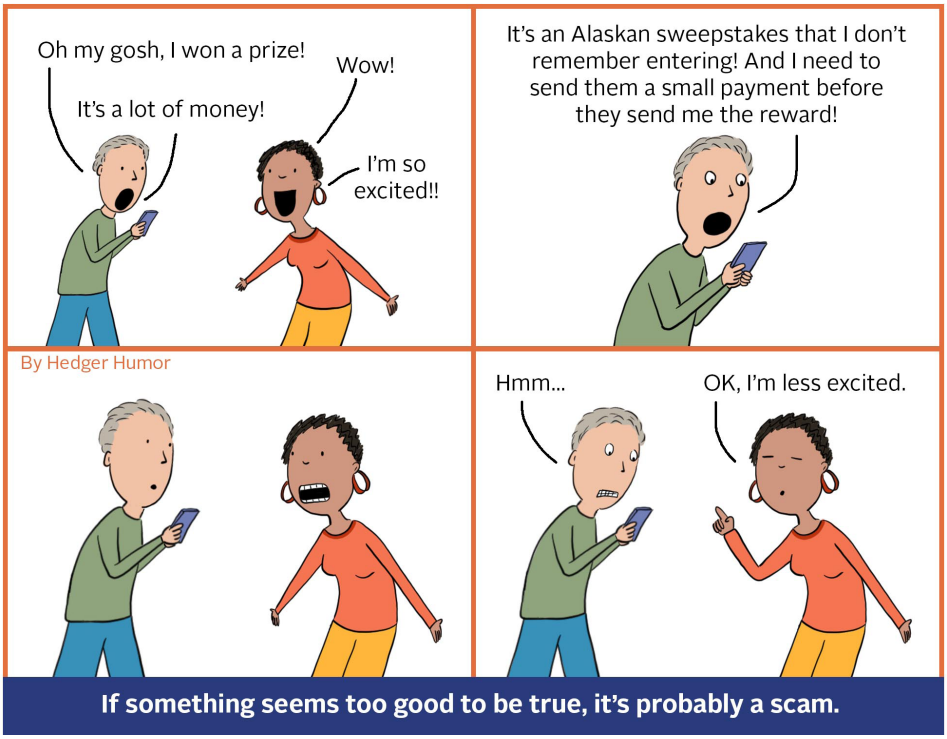
- The message was unsolicited or unexpected.
- The sender tells you clicking on a link or opening an attachment will avoid a negative consequence or gain something of value.
- The email has bad grammar or spelling errors.
- The message promotes a sense of urgency to comply with the request (scammers often intend to make you feel uncomfortable).
- The email asks you to view a compromising or embarrassing picture of yourself or someone you know.

And if you prefer watching to reading, check out A Few Words About Avoiding Phishing Attacks.

Scam Self-Defense: Give that Email Content the Sniff Test

When it comes to the decision to "click or not click," sometimes you have to go with your nose. While administering the sniff test, ferret out hints of impropriety: is there anything "off" about the message? Are you being pressured or rushed? Is the message pandering to curiosity? See below for a stinky example.





If you whiff even the slightest suspicious aroma, ask yourself this: What if click? What if I DON'T click? What if I go crazy not knowing what's behind that link? What if I just drag this faintly fusty message to the trash? And if you're not comfortable with deleting it, try contacting the sender with contact info from *outside* the email message to confirm it's legit. In other words: *think before you click!*

BF Skinner, one of the greatest thinkers of the twentieth century, showed us that rats, pigeons and even people can be conditioned to perform a particular behavior, if the outcome is rewarding. All our internet surfing has conditioned us to respond without thinking – there might be a cute baby animal on the other end of that link! But in your email, make sure you know the sender before you go clicking for that puppy.

Until next time, friends: keep on keeping on ... cybermindfully!

Learn more about Becoming Cybermindful at go.udayton.edu/cybersecurity

THIS PUBLICATION IS PROVIDED BY:

University *of* Dayton
Center for Cybersecurity & Data Intelligence

OHIO CYBER RANGE INSTITUTE