Phish Spotter Checklist

BY CRASHPLAN FOR SMALL BUSINESS

Below are 8 red flags to watch for if (and when) you receive a suspicious email. Become a master phishermon and keep this quick checklist handy at your desk. You never know when bait will hit your email inbox.

1. "FROM" EMAIL ADDRESS
Make sure to cross-check the email domain on any suspicious email. This is the name after the @ symbol in the email address. It should match the name and company of the attempted sender (be on the lookout for minor misspellings!). If you are unsure, try looking up the company's email domain through a search engine.

2. MISSPELLING AND INCORRECT GRAMMAR
As noted above, the name of the sender email address should match the name and company in the signature of the email (if there is no signature, this also may be a red flag). Take a look for any misspellings or incorrect grammar in the body of the email as well. Hackers may use a translation machine that doesn't return perfect grammar or spelling.

3. HYPERLINKS
If you receive an unexpected email to your in box, it is best practice to check all the hyperlinks before clicking on them. Occasionally, both the sender and the body of the email can appear legitimate, but the phish is hidden in the links. If you hover over each link, check if the URL leads to the website you would expect based on the sender. For example, if you receive an email from Bank of America, the hyperlinks should bring you to bankofamerica.com.

4. ATTACHMENTS
This might be the most important rule - do NOT open any attachments until you are 100% sure the sender is legitimate. If the email is indeed a phishing attack, the attachment will contain malware that will be exposed to your computer the second the document is opened. It doesn't hurt to check with your IT team or contact the sender through an alternative channel for them to verify the attachment.

5. URGENCY
Rewards or scare tactics are two common phishing approaches that demonstrate a sense of urgency to get you to click faster. A few examples include offering a monetary reward or demanding account reactivation as soon as possible. Or, by imitating your boss's email address, a phisher can use their authority to scare you into opening a harmful attachment. Either way, take pause before clicking on these "urgent" emails.

6. PERSONAL INFORMATION
Legitimate companies will never ask for sensitive or personal information over email. If any credit card information, social security number, etc, is requested, do not provide it. If you need validation, try calling the company's customer support number to confirm whether the request is legitimate. And be sure to look up the phone number yourself, rather than calling any phone numbers found in the email you received.

7. TIME & DATE
View with caution any emails that land in your inbox outside of business hours. Since phishers may be working in a different time zone than you, their bait could hit your inbox in the middle of the night. This small detail, paired with any other red flags on this checklist, could help you spot a phishing attempt.

8. GUT FEELING
Trust your intuition more than anything. As humans, we are good at picking up deviations to normal patterns in our daily life, especially when they may cause danger to us. If you have even the smallest feeling that the email is not legitimate - even if you can't exactly articulate WHY you feel that way - ask your IT team or MSP. Trust us, they would much rather take a few minutes to confirm a legitimate email than spend days or weeks helping the company recover from a ransomware attack!

If you would like more info on how to recognize and avoid phishing attempts, as well as how to report them, check out the Federal Trade Commission’s website here.

Want to learn more about phishing and cybersecurity? Watch the rest of our “Demystifying Data Security” video series!