With the uptick in ransomware infections that are often instigated through phishing emails, it’s crucial to take proactive measures to help protect yourself and your organization’s security. Having a computer that is up to date and patched makes a big difference in reducing an organization’s overall risk of infection. But being vigilant in detecting phishing emails and educating employees in your organization to also be proactive is a critical step in protection.

Here is a quick top ten list for how to spot and handle a phishing email.

1. Don’t trust the display name of who the email is from.
   Just because it says it’s coming from a name of a person you know or trust doesn’t mean that it truly is. Be sure to look at the email address to confirm the true sender.

2. Look but don’t click.
   Hover or mouse over parts of the email without clicking on anything. If the alt text looks strange or doesn’t match what the link description says, don’t click on it — report it.

3. Check for grammatical errors.
   Anyone can make a typo mistake, but pay close attention to emails with grammatical errors. When crafting messages, scammers may use a spellchecker or translation tool, which will give them the right words but not in the proper context.

4. Consider the salutation.
   Attackers sometimes use a general or vague greeting (e.g., “Dear valued customer”) that fits into an automated template. Or they may leave out the salutation entirely. It’s not always an indicator for a scam, but it can be a clue if something seems off.

5. Is the email asking for personal information?
   Be cautious if an email is asking for sensitive or personal information. You can always call the company’s customer support or navigate to your account on their website to confirm if an action is required.

6. Be careful with attachments.
   Attackers like to trick you with an enticing or seemingly normal attachment that contains malware. Never open an unsolicited email attachment that seems suspicious and call the sender to verify if necessary.

   These emails might try to make it sound as if there is some sort of emergency (e.g., the CFO needs a $1M wire transfer, a Nigerian prince is in trouble, or someone only needs $100 so they can claim their million-dollar reward).

8. Check the email signature.
   Most legitimate senders will include a full signature block at the bottom of their emails. Attackers sometimes use a general or vague greeting (e.g., “Dear valued customer”) that fits into an automated template. Or they may leave out the salutation entirely. It’s not always an indicator for a scam, but it can be a clue if something seems off.

9. Don’t believe everything you see.
   If something seems slightly out of the norm, it’s better to be safe than sorry. If you see something off, then it’s best to report it to your security operations center (SOC).

10. When in doubt, contact your SOC.
    No matter the time of day, no matter the concern, most SOCs would rather have you send something that turns out to be legit than to put the organization at risk.

To learn more about preventing and detecting phishing attacks, visit logrhythm.com