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 truly is. Be sure to look at the email address to confirm the true sender.

2. Look but don’t click.
   Hover over 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 or report it.

3. Check for spelling errors.
   Watch out for tricked out or being grammatically correct than a normal email would be.

4. Consider the salutation.
   Is the address general or vague? Is the salutation “Dear [insert title here]”?

5. Is the email asking for personal information?
   Legitimate companies are unlikely to ask for personal information in an email.

   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 urgent email that they can save their million-dollar reward).

7. Check the email signature.
   Most legitimate senders will include a full signature block at the bottom of their emails.

8. Be careful with attachments.
   Attachmentsfirebase to trick you with a really juicy附件 or file. Don’t open or download anything unless you’re sure it is a file you trust or someone you trust.

9. Don’t believe everything you see.
   Be aware of any unusual or strange attachments. If something looks slightly off or the area, it’s better to be safe than sorry. Open it in a separate window or operations order (viruses).

10. When in doubt, contact your SOC.
   No matter the time of day, no matter the reason, and if you are unsure contact the Security Operations Center (SOC) immediately.

Learn how LogRhythm can help you stop a phishing attack in its tracks.

LEARN MORE