

WHITE PAPER

7 Ways to Recognize Emails Attacks



HOLM SECURITY



Protect Yourself from Phishing Attacks

Phishing is the most common form of social engineering, designed to trick individuals into clicking on malicious links or handing out personal or other highly sensitive information, such as banking information, credit card information, trade secrets, or email credentials. By using one person's credentials, cybercriminals can gain control over even more email accounts that will be used to attack other users. Awareness training is a crucial factor in avoiding most phishing attacks. Don't click on links that are not verified, don't let the urgency get to you, and most importantly, don't hand out personal information or credentials.

Taking Advantage of Wellknown Brands & Events

Phishing attacks often take advantage of our emotions. Phishing scams target our human response. In the wake of the Covid-19 pandemic, phishing emails containing words like "COVID-19 testing", "quarantine," and "vaccine" were used to play on people's concerns and emotions. Cybercriminals use fear as a way to get people to download malicious attachments. It's easy to let emotions and urgency override our ability to assess the email for what it actually is. Cybercriminals also use big brands that you've previously engaged with. It could be a coupon from McDonald's or a package from DHL.

Don't Believe the Urgency

The reason why some phishing scams work is by winning the recipients' trust. It can be by making you think they are someone high up in your organization, stressing the urgency of a banking transfer. Don't get swayed simply because the sender seems to know a lot about you. The sender can project themselves as an insider, as a colleague, or as your manager. Together with information collected from social media profiles and historical emails, they can make phishing emails look authentic.





The Secrecy Tricks

Be cautious if the sender demands total secrecy. Often cybercriminals pose as a board member or manager, asking an employee to transfer funds to a specific account – often claiming it as a matter of secrecy and urgency. These types of emails work because they stress confidentiality, telling you the task is confidential and therefore must not be discussed with anyone else, making you less likely to notice any red flags.

Ask for Help

Cybercriminals often hide malicious content inside innocent-looking document files, where you need to change your security setting to view the content correctly. This might trick you into turning off security features that keep you safe. Here, a second opinion goes a long way. It's the same as asking your colleagues to proofread that important document you're going to send to your manager; they'll find mistakes that you can't believe you missed. Ask a colleague for help if you're not sure if the email should be treated as suspicious or not - two pairs of eyes are better than one.



1. Verify Links

A good rule of thumb is to always verify all links before clicking on them. While both the sender and content can appear legitimate, malicious intent can be hidden in the links. Hover over each link in your email program to verify that the actual address is the same as the link tells you.



2. Verify the Sender

Always verify the sender's email address by hovering over the sender's name or email address. Notice that anyone can say that their name is someone you recognize, but the actual sender's email address is much harder to fake.



3. Be Careful with Attachments

Don't open an attachment until you're 100% sure the sender is legitimate. If it's an email attack, the attachment will certainly contain malware that will be exposed to your computer once the document is opened.



4. Protect Sensitive Information

Legitimate businesses will never ask for sensitive or personal information over email or a website. If any credit card information or other personal information is requested - assume the sender is fake.



5. Misspellings & Incorrect Grammar

Cybercriminals tend to use online translation tools that result in imperfect grammar or spelling. Misspellings and incorrect grammar are common characteristics of phishing emails. Cybercriminals can also intentionally misspell words to minimize the risk of the email being blocked by a spam filter.

90%

of all incidents start
with an email attack.

How Will You Respond?



WHITE PAPER

7 Ways to Recognize Email Attacks



6. Don't Believe the Urgency

Cybercriminals want to scare you into opening a harmful attachment. Don't click on a link just because the sender says it's urgent. They emphasize the urgency cybercriminals make it look like the email was sent in a hurry, from a mobile phone or similar using the signature "Send from my mobile phone." This is a trick to make you more susceptible to things that might look different from the way a person usually expresses themselves.



7. Communicate

If you're still unsure about an email, there's no shame in asking a colleague for help. Perhaps they'll spot something overlooked by you. Or simply pick up the phone and call the sender.



HOLM SECURITY

Phishing & Awareness Training

Over 90 % of data breaches start with a malicious email. Do you know how your users will respond to the next attack? By leveraging simulated email attacks, such as phishing, spear phishing, and ransomware - along with our awareness training tools - we help you increase your resilience against social engineering.

Get Started Today