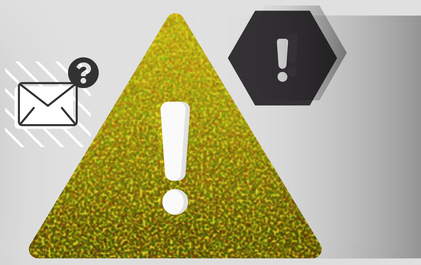
IDAGENT
A Kaseya COMPANY

CAN YOU SPOT THE PHISHING EMAIL?

One of today's biggest phishing risks is email spoofing. In this form of phishing, cybercriminals mimic official corporate communications to lure unsuspecting employees into interacting with them. About **25% of the emails** that businesses receive from major brands like Amazon, Microsoft or DHL are actually fake. Discerning what is real vs. fake could prevent a cybersecurity risk from turning into a cybersecurity disaster for your business.

CHECK THE SENDER'S DOMAIN AND EMAIL ADDRESS

Legitimate companies send emails from their official domain, like "microsoft.com," not variants like "microsoft.business.com." If a domain looks odd, check the address on the company's website.



PAY ATTENTION TO THE HEADER AND FOOTER FOR CLUES

If the header or footer is inconsistent with other messages from that brand, has missing information or is just slapdash, it's likely the message is a phishing attempt.

LOOK AT THE SUBJECT LINE AND PREHEADER

Does the subject line or preheader of a message seem a little "off" to you? Are there odd phrases, emojis or unusual things in the subject line and/or preheader? If yes, it indicates phishing.

FROM: noreply@gmail.com
SUBJECT: OPEN NOW YOU'VE WON!!! 💰💰💰

Congratulations customer,

Your email has been selected. Click to claim your prize now!

https://am@z0nQRfkdjhsjdbgHFULsfjhdsniol88Fb62m

Please refer to attached (PDF FILE) for full prize list.

Regards,
J. Smith

ANALYZE THE CONTENT AND IMPLIED URGENCY

Claiming an action is urgent, offering a special that's too good to be true, or insisting a company must make a payment before services are cut off are each hallmarks of phishing.

BEWARE OF FORMATTING RED FLAGS

This is where many of us catch phishing attempts. If the message has strange formatting, spelling mistakes or bad grammar, or the colors, logos and fonts are "off," it's probably phishing.

BE WARY OF UNEXPECTED ATTACHMENTS LIKE PDFS OR WORD DOCS

If you aren't expecting an attachment or an attachment looks suspicious because it has a strange name, it might be malware or ransomware, which is frequently deployed through phishing.

USE CAUTION IF A MESSAGE ASKS YOU TO LOG IN THROUGH A NEW LINK

Consider the links that a message asks you to click to see if they're going to the company's actual domain or log in on their site directly. Fraudulent password reset requests are a staple of phishing.

IT'S ALWAYS BETTER TO BE SAFE THAN SORRY WHEN IT COMES TO EMAIL HANDLING

Phishing is the most common cyberattack employees will come across. About **80% of reported security incidents** are phishing related. The good news is that regular security awareness training with a solution like BullPhish ID empowers employees to spot and stop bogus messages, such as fake branded emails, and reduces your company's chance of experiencing a damaging cyberattack by up to 70%.

Book a demo of our affordable security awareness training solution BullPhish ID today.

BOOK A DEMO