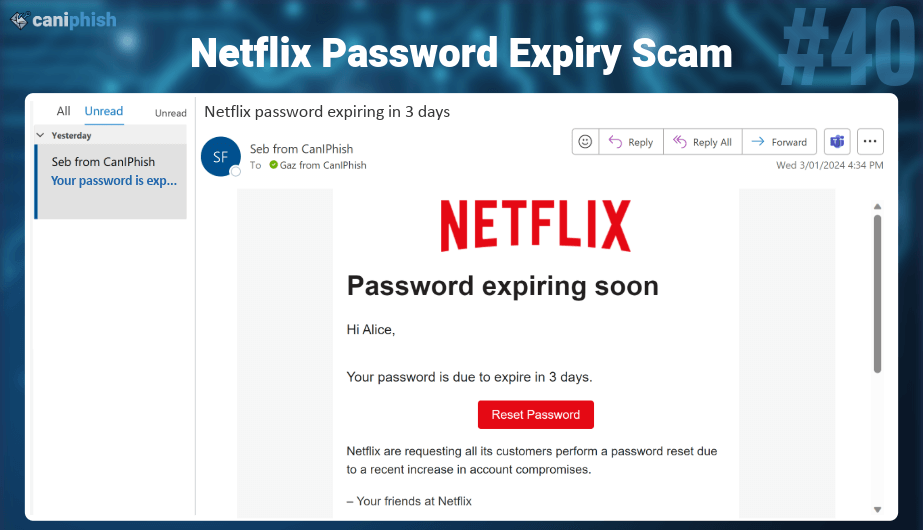
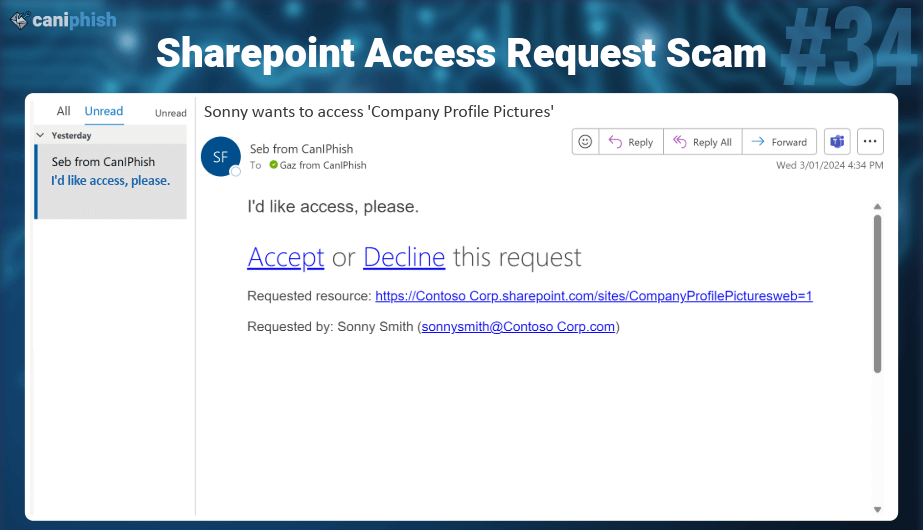
**Netflix Password Expiry**

* **What is this email?** This email claims to be from Netflix, warning the recipient that their password is due to expire soon and urging them to reset it immediately due to a purported increase in account compromises. It includes a "Reset Password" link, which is, in reality, a phishing attempt to steal Netflix login credentials.
* **Why is this email difficult to spot?** The email mimics legitimate security alerts from Netflix, incorporating typical language about account security and urgent action. It uses a direct and personal tone, referring to the Netflix team as "Your friends at Netflix," which can make the communication feel more authentic and trustworthy. The inclusion of standard footer links (Settings, Terms of Use, Privacy, Help Centre) similar to those in genuine Netflix emails adds to the deception, making it appear more credible.
* **Who is prone to falling for this phish?** Netflix subscribers, especially those who may not be aware of how legitimate password reset processes are typically handled, might be susceptible to this phishing attack.



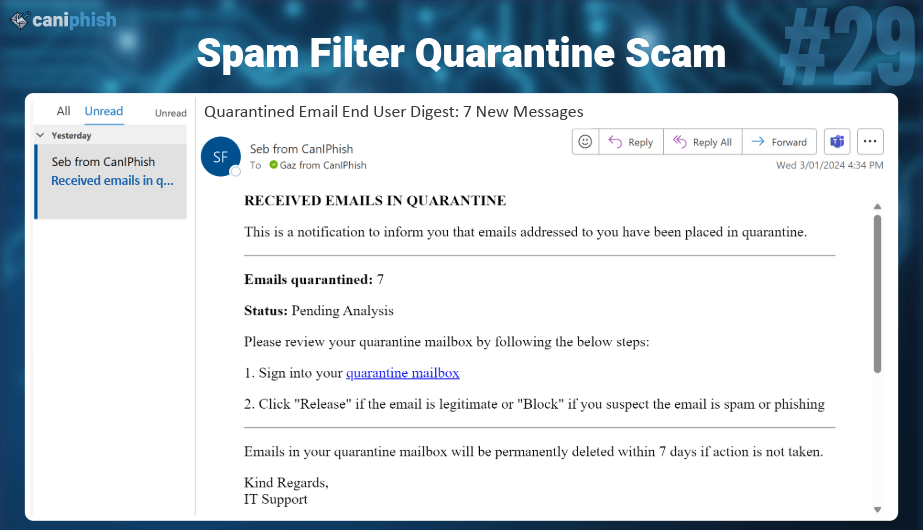
**Sharepoint Access Request**

* **What is this email? This email is a request for access to a SharePoint resource. It provides options to "Accept" or "Decline" the access request and includes details of the bogus requester, Sonny Smith, with an email purportedly from the same company domain.**
* **Why is this email difficult to spot? The email utilizes a common legitimate function of SharePoint—access requests—which employees may regularly encounter in a workplace that uses SharePoint for document and resource management. The format is concise and mimics the style of genuine SharePoint notifications, complete with company-specific URLs and names that add an air of authenticity.**
* **Who is prone to falling for this phish? Employees who frequently use SharePoint in their organizational workflows are particularly vulnerable to this type of phishing attack. Those not vigilant about verifying the legitimacy of access requests or those accustomed to routinely granting such permissions may quickly respond to the email without proper scrutiny.**



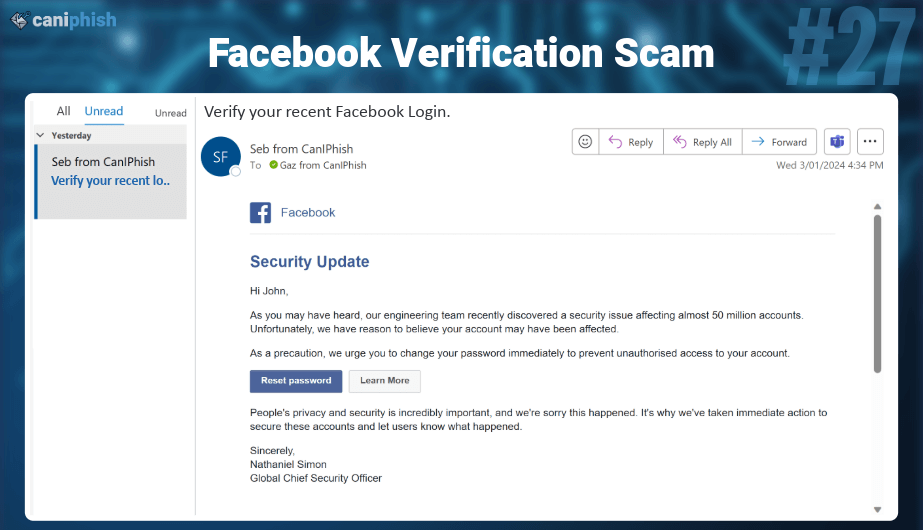
**Quarantined Email**

* **What is this email?** This phishing email masquerades as a notification from the organization's spam filtering software. It prompts employees to sign into their quarantine mailbox to review seven suspected phishing attacks, leveraging a bogus sender profile for authenticity.
* **Why is this email difficult to spot?** Checking quarantined emails is routine, making this email seem like a standard procedure. It also injects urgency by stating that the user has only seven days to act, aiming to rush them into bypassing their usual critical thinking.
* **Who is prone to falling for this phish?** System administrators, particularly those lacking experience or training in detecting phishing attempts, are likelier to fall for this scam. Their familiarity with email security processes can ironically make them less cautious about such seemingly routine notifications.



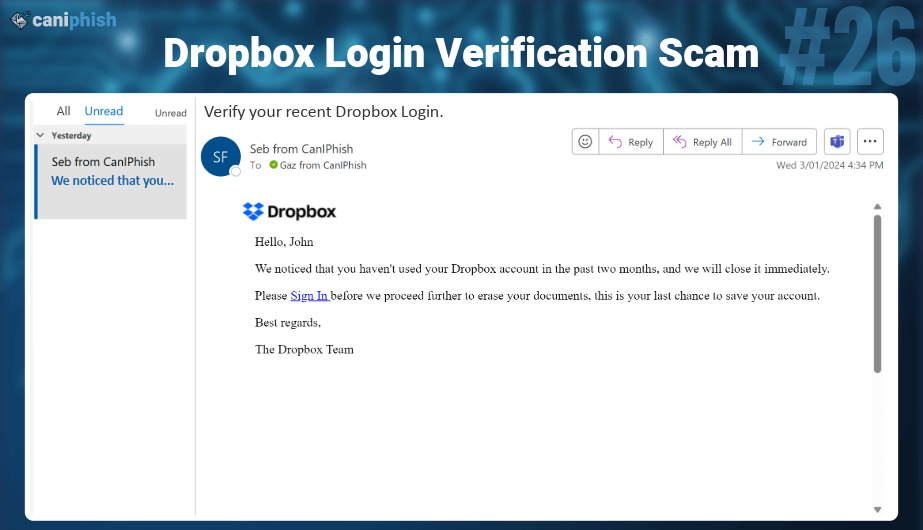
**Facebook Verification**

* **What is this email?** This email poses as an urgent security notification from Facebook, claiming that a significant breach has impacted almost 50 million accounts, including that of the recipient. It insists on immediate action to change the password through a provided "Reset password" link.
* **Why is this email difficult to spot?** The difficulty in identifying this email as a phishing scam stems from its realistic portrayal of a credible security threat—a scenario that Facebook has experienced in the past. The email uses technical language and the name of an authoritative figure within the company, enhancing its legitimacy. Furthermore, the email taps into the recipient's fear and urgency to secure their personal information, which can cloud judgment and lead to hasty actions.
* **Who is prone to falling for this phish?** Any Facebook user, particularly those who are not regularly updated on legitimate security practices or news, might fall for this phishing attempt. Users who are aware of past real security breaches at large companies may be even more inclined to believe the authenticity of the email and follow the deceptive instructions without sufficient scrutiny.



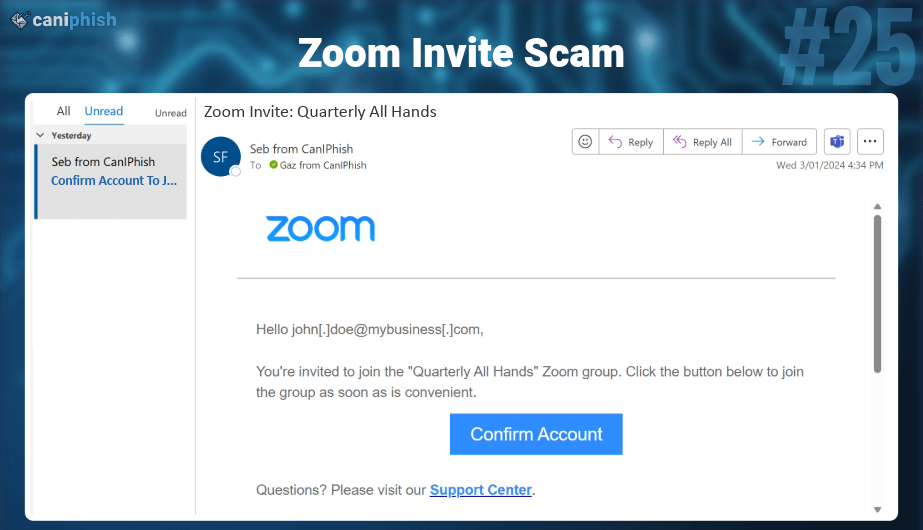
**Dropbox Verification**

* **What is this email?** This email masquerades as an urgent notification from Dropbox, asserting that the recipient's account has been inactive and is on the verge of being closed. It pressures the user to act swiftly to save their account by signing in through a provided link, which is likely malicious.
* **Why is this email difficult to spot?** The difficulty in recognizing this email as a phishing attempt stems from its plausible scenario of account inactivity leading to closure, a policy some real services might follow. The email's professional tone and concise language mirror legitimate corporate communication, making it seem authentic at first glance.
* **Who is prone to falling for this phish?** Individuals who use cloud storage services like Dropbox for personal or business purposes could be particularly vulnerable to this phishing attempt. The urgency conveyed by the threat of losing important documents can prompt hasty actions, especially if the recipient has not recently checked their account activity and fears data loss.



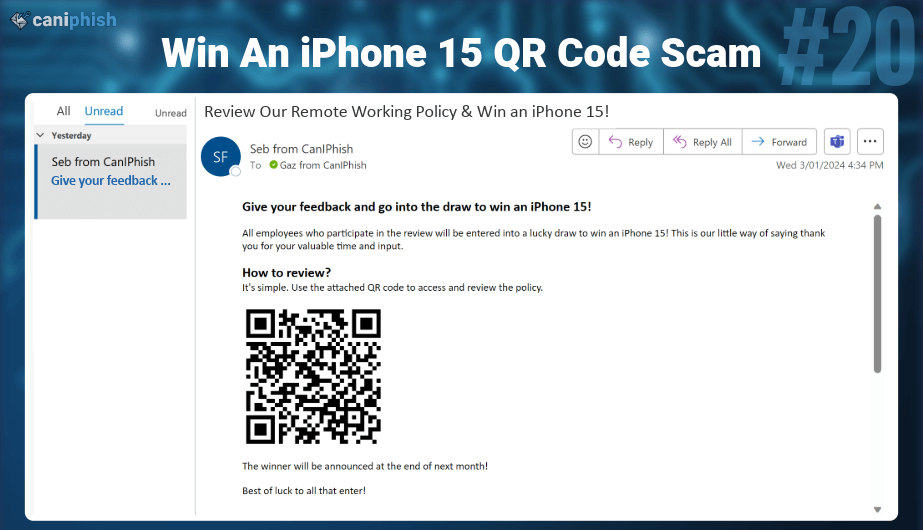
**Zoom Invite**

* **What is this email?** Adopting Zoom's familiar branding, this email announces a "Quarterly All Hands" meeting, urging users to confirm their account. It directs them to a button, which leads to a fraudulent Zoom login page.
* **Why is this email difficult to spot?** Zoom's widespread use across various organizations makes this email seem routine, even for employees whose companies don't primarily use Zoom. Paired with a phony Zoom login page and a subtly disguised sender profile, spotting the deception is challenging.
* **Who is prone to falling for this phish?** Employees accustomed to Zoom meetings, both within and outside their organization, are prime targets.



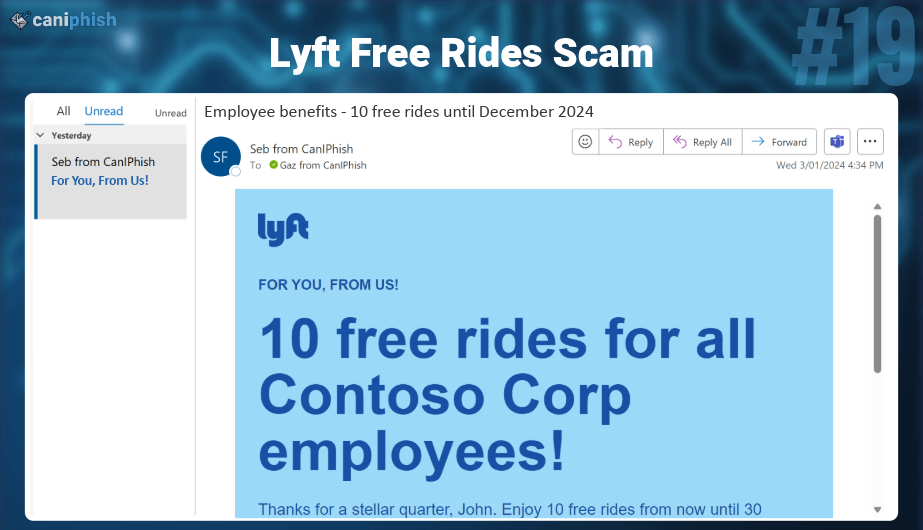
**Win An iPhone 15 QR Code**

* **What is this email?** This email, seemingly from HR, promotes a company competition with an iPhone 15 as the prize. All you need to do is scan the QR code to get started...
* **Why is this email difficult to spot?** An exciting contest combined with the ease of entry via a QR code makes this phishing email particularly convincing. Its expertly crafted appearance and feel closely mimic legitimate corporate communications.
* **Who is prone to falling for this phish?** Employees drawn to the thrill of winning, especially tech enthusiasts eager for the latest gadgets, are most likely to be enticed into scanning the QR code without due caution, making them prime targets for this phishing tactic.



**Lyft or Uber free rides**

* **What is this email? Disguised as a message from HR, this email entices employees with the offer of 10 free Lyft rides as part of a company initiative. Clicking the phishing link leads to a prompt for company login credentials.**
* **Why is this email difficult to spot? Blending a typical company incentive scenario with Lyft's branding, the email convincingly bypasses suspicion for those not well-versed in spotting such deceptions.**
* **Who is prone to falling for this phish? Employees in companies that routinely use Lyft or offer perks like freebies are particularly susceptible to this convincing phishing scheme.**

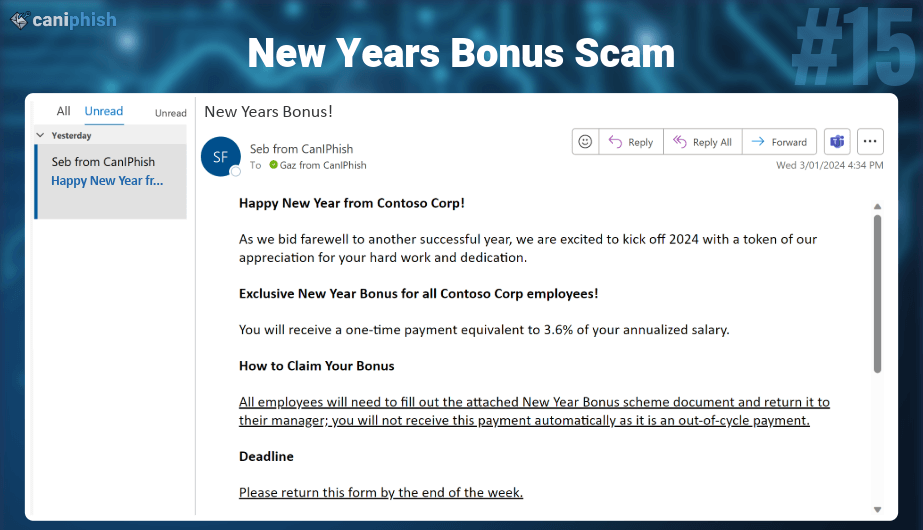


**Fake Meeting**

* **What is this email? Posing as a Google Meet invite, this email tricks employees into clicking a link that leads to a fraudulent site designed to harvest their credentials.**
* **Why is this email difficult to spot? Mimicking a legitimate and familiar format creates urgency with a 'now' timing and includes the employee's email in the body, enhancing its authenticity.**
* **Who is prone to falling for this phish? Individuals who overlook verifying the sender's information are particularly susceptible. Additionally, organizations that frequently use Google Meet as their primary video conferencing tool face a heightened risk of falling prey to this scam.**

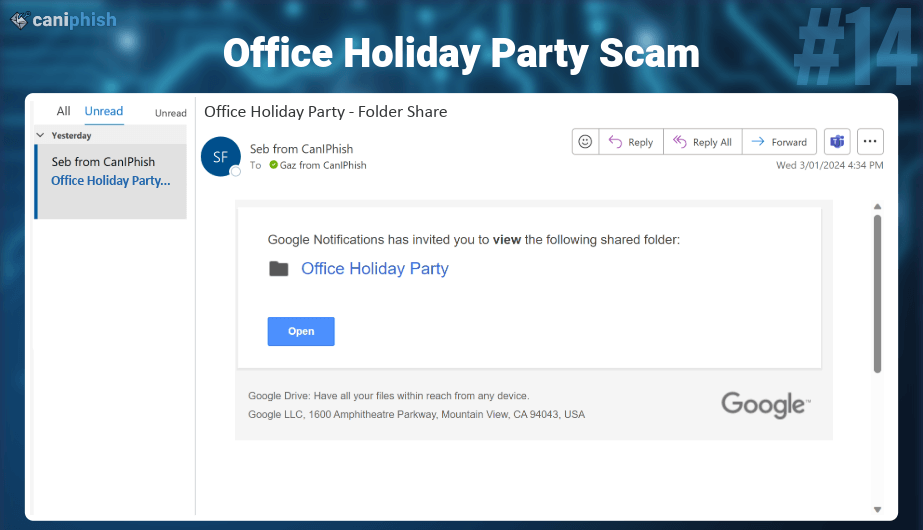
**New Years Bonus**

* **What is this email? This email, disguised as an HR announcement, tempts employees with a large bonus, luring them to complete a form. Its unusual nature doesn't deter 42% of employees, swayed by the cash promise.**
* **Why is this email difficult to spot? This text-based email cleverly uses personalized details, creating urgency and authority. Combined with the promise of financial gain, it embodies classic phishing tactics, making it difficult to spot.**
* **Who is prone to falling for this phish? Employees who don't pause to scrutinize the email's authenticity, especially in their eagerness for the bonus, are most susceptible to this scam.**



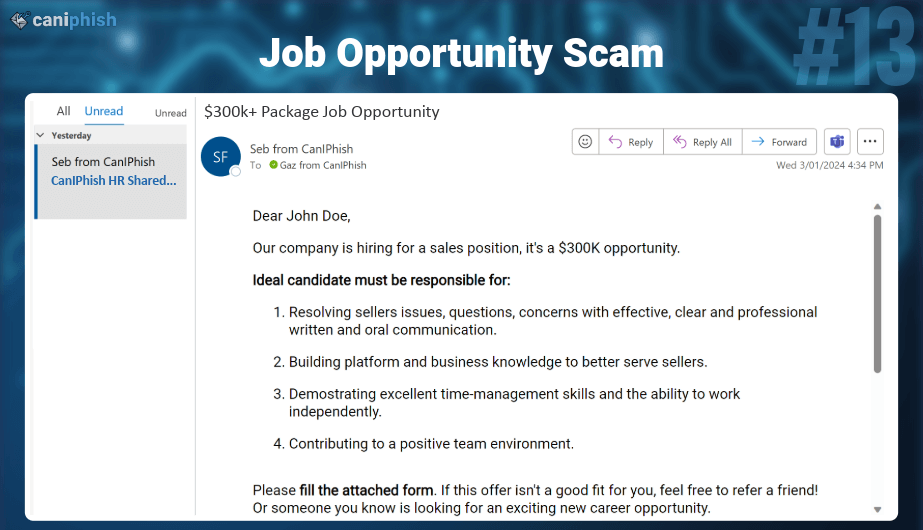
**Office Holiday Party**

* **What is this email? A seemingly innocent email poses as Google Drive, inviting you to an "Office Holiday Party" with a simple "Open" button. Clicking leads to a phishing site aiming to snatch your Gmail credentials.**
* **Why is this email difficult to spot? Leveraging Google's trusted brand and our innate curiosity, this email contains no personalization. Its simplicity and harmless appearance make the email an effective phishing attack.**
* **Who is prone to falling for this phish? Curious individuals, drawn in by the mention of an office party, are most likely to fall for this cleverly disguised phishing attempt.**



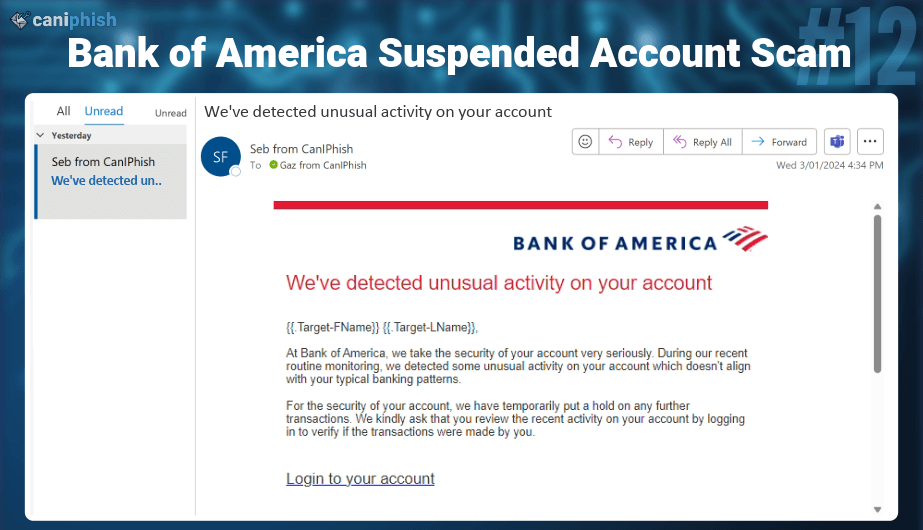
**Job Opportunity**

* **What is this email? Disguised as an offer from HR, this email dangles a job with a hefty salary and generic requirements and asks you to fill out and return an attached file.**
* **Why is this email difficult to spot? The email's cunning lies in its personalization and simplicity, addressing you by your full name, making it seem credible and hard to doubt.**
* **Who is prone to falling for this phish? This email is generic and has proven to be extremely difficult to spot. Any employee curious or motivated by financial gain is prone to falling for this phish.**



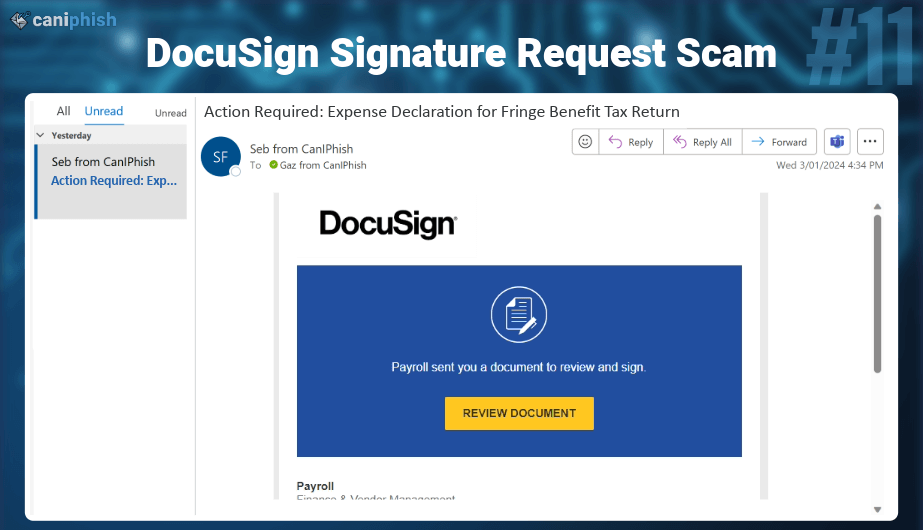
**Bank of America Suspended Account**

* **What is this email? This email is masquerading as a Bank of America suspended account notification. It’s notifying the recipient that unusual activity has been detected on their account, and accordingly, an account hold has been put in place. To remedy this, the email tries to entice the recipient to click a button, which then leads to a phishing website.**
* **Why is this email difficult to spot? This email uses a high degree of personalization, using the recipient's first and last names within the email body. Further to this, it’s easy for this email to mix in with the flurry of legitimate emails that Bank of America periodically sends out.**
* **Who is prone to falling for this phish? Employees who use Bank of America as their banking institution. Typically, this will only be for a subset of employees located in the United States of America.**



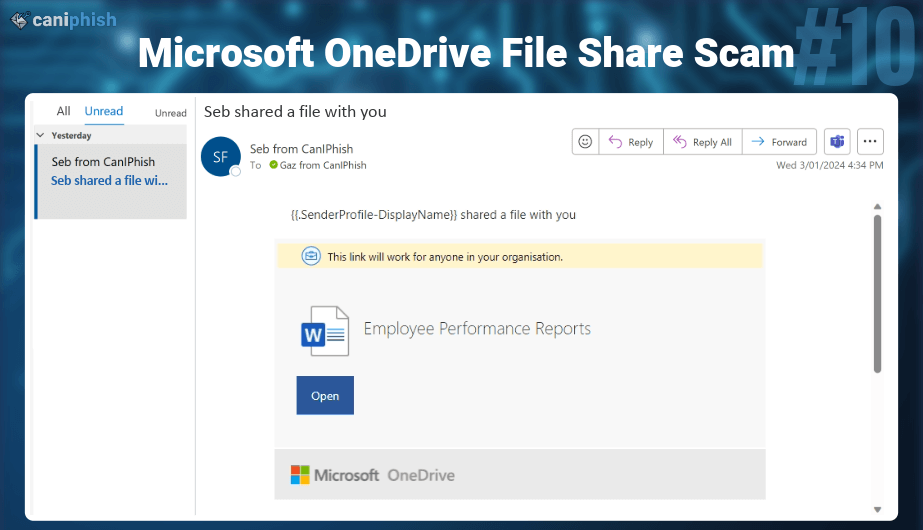
**DocuSign Signature Request**

* **What is this email? This email is masquerading as a DocuSign signature request, where the recipient is asked to click on a link to review and sign a document.**
* **Why is this email difficult to spot? It’s not uncommon that DocuSign signature requests come through at unexpected times. It could be that you need to sign off that you’ve read a certain policy, performed an annual training, or done a variety of other actions. Because of this, recipients of DocuSign emails have become trained to expect unsolicited emails appearing to come from DocuSign.**
* **Who is prone to falling for this phish? Any employee is prone to this phishing email.**



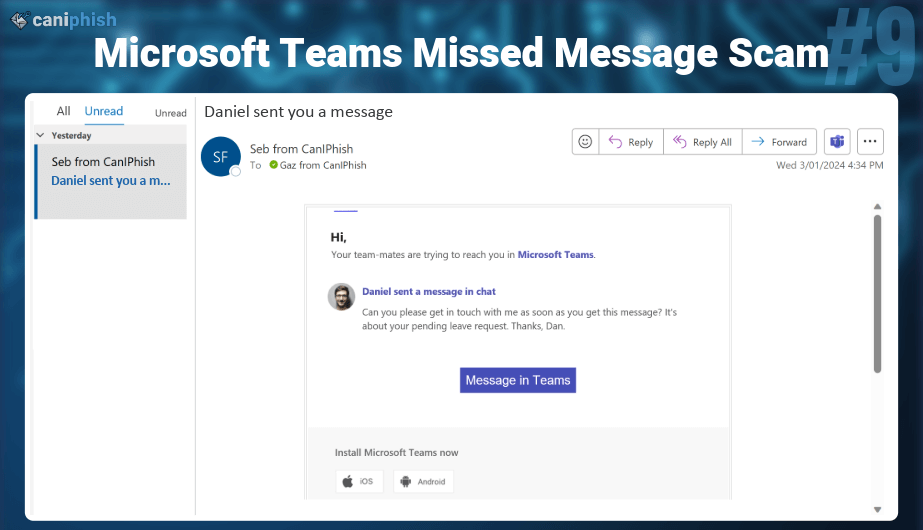
**Microsoft OneDrive File Share**

* **What is this email? This email is masquerading as a Microsoft OneDrive file share email. It notifies the recipient that they’ve just been sent a Word document relating to employee performance reports and prompts the recipient to click a link in the email to view the document.**
* **Why is this email difficult to spot? While this email contains no personalization, it’s trying to invoke an emotional response in the recipient because this file has likely been shared with them by accident and contains sensitive information that they would want to know about. If the recipient is a little bit too curious, they’ll click the phishing link without properly analyzing the email.**
* **Who is prone to falling for this phish? Employees who use Microsoft OneDrive will be particularly susceptible to this email, but because Microsoft OneDrive is frequently used to share files with non-Microsoft users, any employee could be susceptible to this phish.**



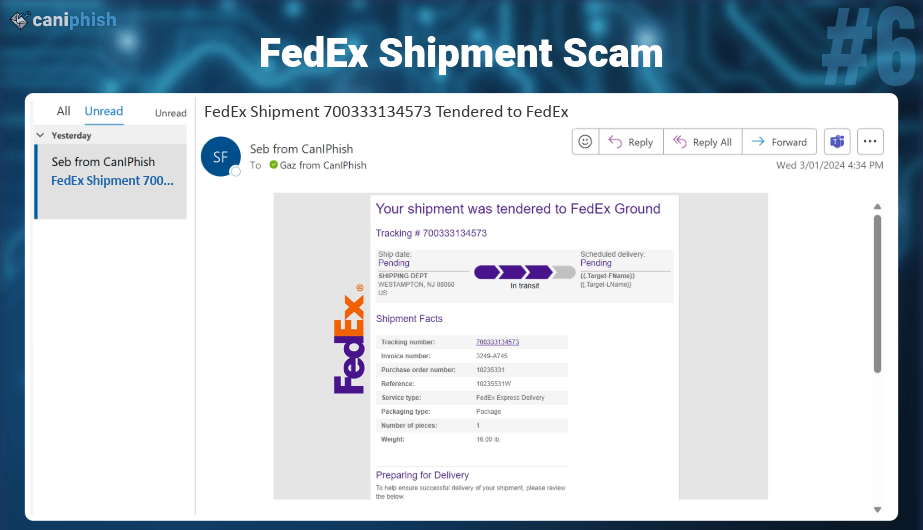
**Microsoft Teams Missed Message**

* **What is this email? This email is masquerading as a Microsoft Teams missed message notification. It’s notifying the recipient that a team member tried to contact them about an upcoming leave request they’ve made. It then prompts the recipient to message the sender back by clicking a button.**
* **Why is this email difficult to spot? When someone is away from their desk or misses a message, it’s common to get an email from Teams keeping them updated on everything that’s happened in their absence. While this email contains no personalization, it fits into the theme of generalized notifications that Microsoft Teams sends out and can easily be overlooked as just another legitimate notification.**
* **Who is prone to falling for this phish? Any employee who uses Microsoft Teams.**



**FedEx Shipment**

* **What is this email? This email is masquerading as a FedEx shipment tracking notification. It advises the recipient that they have a package in transit and entices them to click the tracking link.**
* **Why is this email difficult to spot? It’s not an uncommon scenario that packages are received without prior notification. It could be a present from someone, a gift from an individual's workplace, or perhaps even a delivery that’s just been forgotten. These factors can make a normally unexpected email seem normal. Couple that with some personalization in the form of the recipient's first name, and we have an effective scam.**
* **Who is prone to falling for this phish? Any general consumer or employee is vulnerable to this phish.**



**HR Policy Violation**

* **What is this email? This email is masquerading as an email from the HR team, notifying the receiving employee that they’ve violated company policy and viewed inappropriate material on their work computer.**
* **Who is prone to falling for this phish? Due to the general nature of the phish, any employee could fall for it.**
* **Why is this email difficult to spot? This email can send shivers down the spine of anyone who receives it. It leaves the recipient questioning, what was it that I did? How bad was it? Did I run the wrong search on the wrong computer? In any case, it leaves the recipient with a feeling that they need to prepare their defense, and the first part of that is viewing the purported evidence. Adding an additional layer of deviousness, this email contains a phishing link, a phishing attachment, and a high degree of personalization.**

