Recognize & Avoid Phishing

Phishing emails are the primary attack method in the cyber criminal's playbook. These attacks try to trick you into taking an action, such as clicking a link, opening an attachment or responding with sensitive information. We're all a target, both at work and at home, because our information – and our devices – are worth good money to cyber criminals. Read on to learn how to spot phishing so you don't take the bait!

PRACTICE SAFE EMAIL BEHAVIOR

It's important you understand what is safe and not safe when processing email in your inbox.

It's SAFE to:

✅ Open and read an email
✅ Preview an email in the reading pane of Outlook
✅ Delete or ignore an email

Do NOT:

X Open attachments or click on links
X Preview an attachment or link in Outlook – that's just like opening it
X Reply to or provide information back to the sender

IDENTIFY THE RED FLAGS OF PHISHING

These are the most common identifiers associated with phishing attempts. Use these red flags to review all external email:

√ **Weird or unknown email address.** If the email descriptor or the signature in the email says it's from a company, but the email address looks completely different, it's likely not a legitimate email. This is the best way to tell if an email is suspect.

√ **Blank or "undisclosed" recipients.** Sometimes phishing emails are sent to a lot of people. Other times you see something like "undisclosed recipient list" in the "To:" field. Both of these are potential red flags.

√ **Lack of personalization.** Did the email use a generic salutation such as 'Dear Customer' or nothing at all? Service providers usually know who you are and typically personalize emails with your name and the last few digits of your account number.

√ **Bad spelling and grammar.** Legitimate businesses go out of their way to proofread their email. If an email has lots of spelling mistakes or improperly worded sentences, it's likely a phish.

√ **Urgent request.** Messages of an urgent nature, or requesting an immediate call to action, are a common method used to rush people into making mistakes, and is another good indicator of phishing.

Recognize & Avoid Phishing

√ **Strange website links.** If you hover your mouse over a website link, you will see the actual destination of the website you're about to visit (on some mobile devices you can accomplish the same thing by holding your finger on the link for a second or two). If that location differs from the way the link is written in the email, it's a good indication of an attack.

√ **Suspicious attachments.** If you don't know the sender, or receive something from a friend that looks suspicious, don't open the attachment. If it is from someone you know, you can always pick up the phone and give them a quick call to make sure they actually sent the email.

√ **Requests for sensitive information.** Be suspicious of requests for sensitive information, such as user IDs and passwords, financial account numbers, health information or social security numbers.

ADVANCED TECHNIQUES TO IDENTIFY PHISHING ATTEMPTS – EXTERNAL

- Do an online search to make sure a company exists and the contact information they provide – like address and phone number – is correct.

- Try to do an online people search via LinkedIn or Google to verify that the person sending the email works at the company listed. For emails that look like they came from someone at Nationwide that you don't know, check our online directory.

- Navigate the company's website in a browser to see if the URLs in the email match up. If they do, then the email is likely safe.

- If you do business with the company, use your own contact information to verify that the email you received is legitimate. Call them directly!

- Ask someone you know at work if they know the company and/or person who sent you an email.

TIPS AND TRICKS WHEN EMAILING WITH EXTERNAL PARTNERS

Some of us rely on external partners to do our jobs, making it hard to identify phishing attempts. We understand, and have come up with some tips and tricks that you can use in your area to make it easier to spot legitimate, external email from partners.

- Keep a comprehensive list of external partners and contact information. Make sure it is accessible to anyone who may receive email correspondence so they can double check email addresses, senders, and the type of business they conduct with Nationwide.

- Add frequent external partner email addresses to your address book. This will make sure legitimate emails are delivered to your inbox, and not be flagged as Promotional or Junk Email.

- Verify an email, attachment or urgent request by phone. If you’re not expecting an email from an external partner, pick up the phone and call them to verify what they need.

- Create operational procedures that make it easier to spot legitimate, external emails. For instance, make sure all outgoing emails contain identifiers that can easily be looked up – like a partner identification number, claim number, account number, etc. Ask external partners to follow a system as well.