LINDENWOOD
UNIVERSITY

Phishing emails

These emails are a threat to our online safety, so it's crucial we learn how to recognize them. Here's a quick guide to help you identify phishing emails:

- Check the Sender's Email Address: Pay close attention to where the email is coming from. Be cautious of emails from addresses you don't recognize or that look a bit strange. Cybercriminals often try to make their addresses look like real ones.
- Is This Expected? If you get an email about something unexpected, like a package or special instructions, it's a good idea to double-check. Reach out to the person through a different method, like calling or in person, to confirm.
- Look at the Salutation: Legitimate emails from real organizations usually use your name. Be careful if the greeting is generic, like "Dear Customer" or "Dear User."
- Watch for Urgent Language: Phishing emails often try to make you feel rushed and pressured to do something right away. If you're asked to urgently give sensitive info or click a link, be cautious.
- Hover Over Links Before Clicking: Move your mouse over any links in the email without clicking. Check if the web address matches what's shown. Be wary if they don't match.
- Check for Mistakes: Phishing emails often have spelling or grammar errors. If the language looks off, it's a sign it might be a phishing attempt.
- Avoid Sharing Sensitive Info: Real organizations usually don't ask for sensitive info (like passwords or Social Security numbers) through email. Don't share this kind of data in an email.
- Be Careful with Attachments: Don't open attachments unless you're expecting them or have confirmed with the sender. These attachments can be malicious.
- Verify Money or Gift Card Requests: If you get an email asking for money or gift cards, be cautious. Confirm with the person through another way before doing anything.
- Look at the Logo and Branding: Phishing emails often have fake or low-quality logos. Compare them to official messages from the organization.
- Trust Your Gut: If something doesn't feel right, trust your instincts. If you're unsure about an email, reach out using official contact info, not what's in the suspicious email.

Remember, knowing about phishing is one of the best ways to protect yourself. If you come across a suspicious email in your email account, report it right away. Your awareness and caution are important for keeping your digital space safe.
We are committed to keeping LU secure. Our team is always working to protect against digital threats. Thanks for being a part of our cybersecurity efforts! For more info on phishing, visit Phishing - National Cybersecurity Alliance (staysafeonline.org)