NWU® | Information Technology

User Guide: IT Services

Phishing Attemps

Learn how to protect yourself from phishing attempts that can include dangerous links and attachments.

1. VERIFY THE SOURCE

Attackers are always coming up with new and inventive ways to trick you into downloading malicious files like ransomware or giving up your password on phishing sites. Sometimes these attempts are obvious, but they are often hard to spot.

2. ATTACHMENTS: ALWAYS CHECK FOR LEGITIMACY FIRST

Spear phishing emails rely on you—they want you to click a link or open an attachment. But before you do anything, you always need to check an email's content for legitimacy. Hover over a link and see if it's going to a reliable URL. Or, if you're unsure about an email's content or the source it came from, do a quick google search and look for other instances of this campaign and what those instances could tell you about the email's legitimacy.

3. IS THE SITE SECURE?

Another way to help verify that a website is legitimate is by looking for a padlock icon in your browser's address bar, which indicates that your connection is secured using HTTPS. Note that HTTPS alone does not make a website genuine—criminals can use encryption, too—but a website without HTTPS is a red flag, especially if it's supposed to be a banking site.

4. SWITCH PLATFORMS

If you receive a suspicious message from someone you know, including a note asking you to respond to an emergency immediately, double-check to make sure it's genuine. You can do that by contacting the apparent sender through another channel since an attacker is far less likely to access multiple accounts. If it's a company, check with it directly to see if the message or site you've been sent is legitimate.

5. REPORT SUSPICIOUS EMAILS

Please log a ticket using our online support portal.
https://support.nwu.ac.za
"Something is not working" > "Cybersecurity Issue" > "Phishing Attempt Issue"

6. WHY IS THIS IMPORTANT

Attackers are always trying new and inventive ways to trick you into downloading malicious files like ransomware or giving up your password on phishing sites. Sometimes these attempts are obvious, but they are often hard to spot.

More on Cyber security info You may use this link

http://services.nwu.ac.za/information-technology/cyber-security-news

- Many fake websites are very carefully designed to look legitimate, and phishing emails can appear to come from someone you know.
- In one example of phishing, scammers send emails designed to look like the IRS sent them. The emails ask for detailed personal information, passwords, PINs, and other information to trick consumers into disclosing their personal and financial data. The scammers then use that information to steal consumers' identities and financial assets.
- Other common scams include con artists creating online identities to trick people into faux romantic relationships and then hitting the victims up for money, identity thieves posing as an individual's friend, and asking for cash for a fabricated emergency.
- Scammers ask to deposit money in people's bank accounts in exchange for a money order—but then they spend the money and don't deposit money (or receive a refund). These phishing attempts can usually be prevented if you're aware of them and know what to look for.

SOURCE | https://securityplanner.consumerreports.org/tool/protect-yourself-from-phishing
https://www.mcafee.com/blogs/privacy-identity-protection/spear-phishing-attacks/