

HOW TO PROTECT YOURSELF AGAINST PHISHING EMAILS

Don't click on that email!
Find everything you need to know in this phishing infographic including how to protect yourself from cyber attacks.

What is phishing? Phishing is an email fraud method where the attacker sends out emails, usually appearing to come from a legitimate website or company, in an attempt to gather personal and financial information from the victim.

Top Causes of Data Breaches

THEFT OR LOSS	HACKERS	ACCIDENTAL INFO LEAK	FRAUD	INSIDER THEFT	UNKNOWN
36%	25%	30%	3%	2%	5%

Signs of a Phishing Attack

- Message from an unknown sender
- Unclear or mismatched link
- Message with poor spelling/grammar
- Unexpected or non-business related call or message
- Message or call asking for private info or containing threats

Tips to Avoid Attackers

- Do not give away any personal information. Most business will never ask for user names and passwords via email.
- Assume that all unexpected emails with a call to action to confirm information, such as clicking a link or downloading a document, are phishing.
- Update your computer's anti-virus software and enable browsers' phishing filters.

Most Targeted Companies

PayPal, eBay, Amazon, Facebook, Bank of America, Google, LinkedIn

Need more help?

Should you experience an IT related problem please log a fault within the *Service Request Manager* or contact your campus IT Service Desk.

Should you wish to provide us with feedback, feel free to drop us an email at talk2IT@nwu.ac.za

Source: https://thumbnails-visually.netdna-ssl.com/what-you-should-know-about-phishing-malware_558d80c1008d8_w1500.jpg