What are phishing scams and how can I avoid them?

- Phishing explained
- Specific types of phishing
- Avoiding phishing scams
- Warnings
- Reporting phishing attempts

Phishing explained

Phishing scams are typically fraudulent email messages appearing to come from legitimate enterprises (e.g., your university, your Internet service provider, your bank). These messages usually direct you to a spoofed web site or otherwise get you to divulge private information (e.g., passphrase, credit card, or other account updates). The perpetrators then use this private information to commit identity theft.

One type of phishing attempt is an email message stating that you are receiving it due to fraudulent activity on your account, and asking you to "click here" to verify your information.

Phishing scams are crude social engineering tools designed to induce panic in the reader. These scams attempt to trick recipients into responding or clicking immediately, by claiming they will lose something (e.g., email, bank account). Such a claim is always indicative of a phishing scam, as responsible companies and organizations will never take these types of actions via email.

Specific types of phishing

Phishing scams vary widely in terms of their complexity, the quality of the forgery, and the attacker's objective. Several distinct types of phishing have emerged.

Spear phishing

Phishing attacks directed at specific individuals, roles, or organizations are referred to as "spear phishing". Since these attacks are so pointed, attackers may go to great lengths to gather specific personal or institutional information in the hope of making the attack more believable and increasing the likelihood of its success.

The best defense against spear phishing is to carefully, securely discard information (i.e., using a cross-cut shredder) that could be used in such an attack. Further, be aware of data that may be relatively easily obtainable (e.g., your title at work, your favourite places, or where you bank), and think before acting on seemingly random requests via email or phone.

Whaling

The term "whaling" is used to describe phishing attacks (usually spear phishing) directed specifically at executive officers or other high-profile targets within a business, government, or other organization.

Avoiding phishing scams

DICTS does not use email to request that you reply with your passphrase or confidential personal information. Be suspicious of any email message that asks you to enter or verify personal information, through a web site or by replying to the message itself. Never reply to or click the links in a message if you are unsure about the source of the message. If you think the message may be legitimate, go directly to the company's web site (i.e., type the real URL into your browser) or contact the company to see if you really do need to take the action described in the email message.

When you recognize a phishing message, delete the email message from your Inbox, and then empty it from the deleted items folder to avoid accidentally accessing the web sites it points to.

Always read your email as plain text.

Phishing messages often contain clickable images that look legitimate; by reading messages in plain text, you can see the URLs that any images point to. Additionally,

when you allow your mail client to read HTML or other non-text-only formatting, attackers can take advantage of your mail client's ability to execute code, which leaves your computer vulnerable to viruses, worms, and Trojans.

Warnings

Reading email as plain text is a general best practice that, while avoiding some phishing attempts, you won't avoid them all. Some legitimate sites use redirect scripts that don't check the redirects. Consequently, phishing perpetrators can use these scripts to redirect from legitimate sites to their fake sites.

Another tactic is to use a homograph attack, which, due to International Domain Name (IDN) support in modern browsers, allows attackers to use different language character sets to produce URLs that look remarkably like the authentic ones.

Reporting phishing attempts

- If the phishing attempt targets Makerere University in any way (e.g., asks for Makerere University Webmail users to "verify their accounts", includes a malicious PDF directed to university human resources, or impersonates Makerere University or DICTS), forward it with full headers to DICTS `helpme@dicts.mak.ac.ug`; for help.