UNITED NATIONS
HUMAN RIGHTS
OFFICE OF THE HIGH COMMISSIONER

OHCHR digital security tips series for human rights defenders in South-East Asia

11 Phishing attacks

A phishing attack is a form of a cyberattack that tricks its victims into trusting the attacker's message (via email, SMS, instant messaging or any other medium) and encouraging specific actions such as clicking a link to a page, downloading an attachment, or logging into a fake website. Phishing attacks can be sent from your colleague' accounts if they have been compromised. It is important to know how to identify phishing attacks to avoid errors that can cause sensitive security breaches.

DO

It is recommended to check the sender's email address. Phishing attacks may contain wrong spellings in the email address to make it look like the legitimate email address it is trying to mimic.

It is recommended that you use a separate channel to cross-check on what is happening with the person who has supposedly asked for your action or information before you act.

It is recommended to have a good separate backup and two-step authentication.

It is recommended to log-out of all unused accounts. In the long term, delete accounts that you don't intend on using.

It is recommended to use a password manager to create and securely store your passwords.

It is recommended to always check for misspellings, grammatical errors, or contextual errors. Phishing attacks often contain misspellings, grammatical errors, or contextual errors in the message subject, body, or signature. A contextual error could be receiving a strange request from a colleague. It is better to check with the colleague before clicking on anything within the email. It is also recommended to check for attempts of getting private or valuable information (passwords, accounts numbers, names, ID numbers, etc.) either through email, text chat, voice call, or a physical visit. Also be wary of messages that evoke urgency or an attempt to evoke an emotional reaction. Social engineering tactics often use emotional manipulation to get people to act in favour of the attacker's agenda.

It is recommended to check the email headers. Email headers contain significant information about the email senders, their address and the servers used to send the email message. Check the "received from:" value and see if it matches the user@email.com domain name. If it does not match, it is more likely a phishing email.

It is recommended to always hover the mouse cursor over hyperlinks[1] to view the destination site. Phishing attacks often include hidden or short links which need to be examined carefully to determine where the link will take you.

It is recommended to check the status or reputation of suspicious websites or links. Using tools such as virustotal.com, hybrid-analysis.com, and urlscan.io. try to scan the reputation of the links or websites that you find suspicious. Note that if it shows "clean," it does not mean it is safe to proceed. Seek further advice if you are still in doubt.

It is recommended to confirm any requests for financial transactions. If there is any financial transaction request in an email, confirm this with the person requesting the transaction either by sending a message from another secure communication channel. If the request came from an institution, ask the person for their name and then try to find the person's phone number of that institution and call the front desk, asking them to patch you through. This way you can avoid falling for spoofed phone numbers.

It is recommended to ask for help. If you are in doubt about a certain email message. Ask for assistance from your colleagues, IT support or third-party technical support contact.

DON'T

It is not recommended to publicly expose your email addresses. Threat actors find all information about their target online. If you have publicly shared or published your information including your email, attackers may use it to perform phishing attacks.

It is not recommended to click any link from an unknown email sender, instead type the address yourself in the address bar. Threat actors may use regular email for phishing attacks. Any unknown sender might send you intriguing messages or anything that may be relevant to your work or research. Do not click any links right away.

It is not recommended to download any attachments from unknown sources. Attachments are commonly also used to compromise the computer of a target user. This can be in the form of excel, pdf, or word documents. Files ending with .bat, .cmd, .exe will not be shown unless a setting is first enabled in Windows allowing you to see the file extensions. Attackers can try to trick you to run an executable file by putting an Excel icon to it which may lead you to believe it is an Excel file even though it's an exe file. If in doubt, ask for help.

It is not recommended to divulge any internal information to unknown senders. Threat actors may use phishing attacks to simply gain information. By asking for information about the organization such as schedule, staff, services, or other information that may seem common to us, but to them, it can be used to perform cyberattacks.

Checklist for detecting Phishing attacks

Since we interact with emails daily, knowing which emails are malicious and which emails are not, is critical to keep our security intact. According to the security company f5, since the COVID-19 pandemic started, phishing attacks have increased by 220 percent.[2]

TIPS!

Signs of a phishing email attack:

Fake or misspelled email address.
- Look at the email address that is sending you the email. If it is not an official email address, or one that tries to look like a legitimate one, delete and do not click on any links or attachments.

Impersonalized emails e.g., Emails with generic greeting such as "Sir/Madam."
- Since most phishing attacks are sent to multiple targets in one message, attackers are using template-based emails to lure users to act/do something.

Requests for personal information.
- Phishing emails may come in the form of job recruitment or job offers, where they ask for personal information such as your phone number, birthdate, educational history, and other information that is typically asked during a hiring process.

Buttons with wrong hyperlinks or back link.
- Use your cursor to mouse/hover to buttons, images and text that may contain links to see they point you to the right domain.

Wrong spelling and grammar mistakes.
- Threat actors use ready templates when they send phishing emails in bulk, which are poorly written and contain confusing grammar.

[1] Hyperlinks can be added to graphics and other media in addition to text.
[2] Security company f5, https://www.f5.com/company/news/features/phishing-attacks-soar-220--during-covid-19-peak-as-cybercriminal.