



- Never share your password(s) with anyone, even if requested by a colleague or your line manager.
- Never send any documents classified as (Internal, Restricted or Highly-Restricted) to the personal email address of an employee or an unauthorized external party for any reason. This will result in the execution of disciplinary actions based on HR Consequence Management.
- Do report security breaches immediately to the Cybersecurity Risk Department using the reporting channels.
- Do lock your workstation when not in use and shut it down at the end of shift.
- Do not post SAB data on social networking sites. It can be misused by strangers!!
- Classify information as Public, Internal, Restricted or Highly-Restricted and label it appropriately.
- Follow Information Security policies strictly. Remember, non-compliance may lead to disciplinary action.
- Do not store work related data on your desktop, as it may be lost. Always store it on department shared drives.
- Sharing bank data with unauthorized parties will lead to disciplinary action. Remember... all emails are being monitored.
- Be caution of phishing websites Learn how to protect yourself against phishing attacks.

- لا تقم أبداً بمشاركة كلمة المرور الخاصة بك مع الآخرين حتى لو طلب ذلك من قبل مديرك أو أحد زملائك.
- لا تقم بإرسال أي وثائق أو معلومات أو بيانات خاصة (الأول) إلى بريدك الشخصي أبداً ... حتى إن كنت تريد العمل من المنزل. لا تقم بإرسال أي وثائق متعلقة بالأول مصنفة كـ (داخلية ، محظورة أو محظورة جداً) إلى بريدك الشخصي حتى لو كنت تريد العمل من المنزل، وأيضا حتى لو كان يعلم مديرك المباشر أو موافقته، هذا التصرف لن يكون مقبولا أبداً وسوف تتخذ إجراءات تأديبية مناسبة ضد الموظف.
- قم بالتبليغ فوراً عن الخروقات الأمنية والأنشطة الإحتيالية لإدارة أمن المعلومات.
- قم بتأمين كمبيوترك في حال عدم إستخدامك له ، وقم بإغلاقه في حال تم الإنتهاء من العمل.
- لا تقم بمشاركة معلومات الأول في مواقع التواصل الإجتماعية. بالإمكان أن يساء إستخدامها من قبل الغرباء.
- صنف المعلومات Public, Internal, Restricted, Highly-Restricted وعلى غرار ذلك قم بوضع العلامة المناسبة.
- إتبع سياسات أمن المعلومات بدقة. تذكر قد يؤدي عدم الإمتثال للقوانين لإجراءات تأديبية.
- لا تخزن ملفاتك على الكمبيوتر الشخصي ، حيث بالإمكان فقدانها. دائماً خزنها على المحركات المشتركة.
- لا تقم بإرسال معلومات الأول لجهة غير مصرح بها أو إلى بريد مجاني Hotmail, Yahoo, Gmail. تذكر جميع المراسلات تخضع للمراقبة.
- كن حذراً من مواقع التصيد الاحتيالي وكيفية حماية نفسك من الهجمات

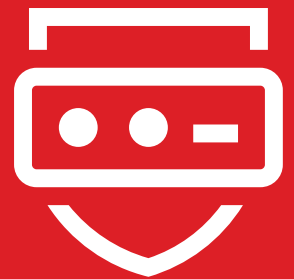


Think before you click

Phishing, smishing, and vishing are techniques used by cybercriminals to obtain personal and confidential information by tricking you into revealing usernames, passwords, sensitive company information, and other personal details via email, text message, or phone call.

Strengthen your passwords

Strong passwords are a simple and effective way to prevent unauthorized access. Your laptops, computers, tablets and smartphones contain a lot of personal data and access details to your online accounts. Creating strong passwords and keeping them secure is key to the security of your information.



Report anything suspicious

Information breaches can have a very serious impact on our business and our reputation. The sooner you report an incident, the quicker our security teams can react. Even if you are unsure, always report anything you think is suspicious. You will not be wasting anyone's time.



Report Phishing



Report by using the Phishing ICON

Hotline: +966 11 2764004



SAB Report Incident on Intranet



Phishing

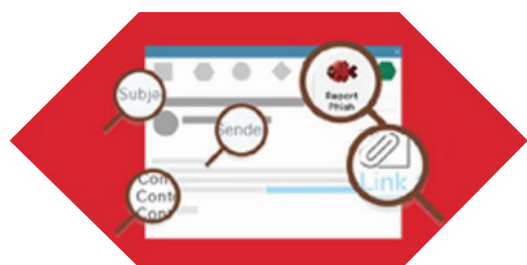
Phishing is a technique used to gain personal and confidential information by tricking you into revealing information such as usernames and passwords, sensitive company information and personal details. Attacks may occur by email, text, or phone. Phishing is also used to spread malware by installing codes into your system to steal information without your knowledge.

Don't give out personal details over email such as bank account details or passwords. Your bank wouldn't ask you to.

Don't make yourself a target. Information you share online on sites like Facebook and LinkedIn can be used to create targeted attacks or guess your passwords. Share responsibly.

Don't open attachments from unknown senders. Verify the sender first by checking the global directory or asking your Line Manager for vendor details.

Do learn to spot the signs of phishing.



Spot the signs of phishing

Check the subject

Look out for the EXTERNAL warning. It informs you that the email is from an external source and should be treated with extra caution. Ensure the subject matches the email content.

Check the sender:

Verify the sender by checking SAB directory or independently confirming that the email address is legitimate.

Check the content:

Look out for warning signs in the email such as:

- urgency or threatening language
- requests for personal or sensitive information
- bad grammar and typos
- replies to messages you never sent



Smishing

Smishing is a social engineering attack that uses fake mobile text messages to trick people into downloading malware, sharing sensitive information or sending money to cyber criminals.

TOP TIPS

- Don't** click on any unknown messages with links in them.
- Don't** reply to text messages asking about your personal financial information.
- Don't** respond to unrecognized text messages or messages from unknown numbers pressuring you to reply quickly.
- Don't** call back numbers associated with unrecognized or suspicious text messages.



Spot the signs of smishing

Your personal information

The criminals are asking you for sensitive or personal financial details.

Urgency

You are led to believe your money is at risk unless you act immediately.

Phone spoofing

The number of the caller appears as if it is coming from somewhere else so you believe the caller is genuine.

Contact

You are asked to call a number to resolve the request.

Holding the line

You are asked to click on a link to resolve the request

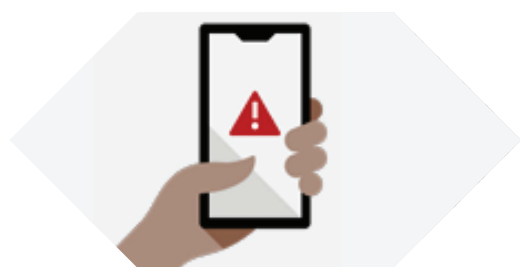


Vishing

Vishing (voice or VoIP phishing) is a type of cyber attack that uses voice and telephony technologies to trick targeted individuals into revealing sensitive data to unauthorised entities.

TOP TIPS

- Don't** give out details and never share credentials such as card details expiry date, CVV, PIN or your mother's maiden name.
- Do** validate the source - if suspicious, independently research the source, DO NOT use the contact details within the call or message.
- Do** be mindful how you describe your role or share personal information on social media. Strengthen your privacy settings.
- Do** be vigilant. If you are suspicious, make a note of the caller ID, the details of the call and any call back numbers.



Spot the signs of vishing

Your personal information

The criminals already have your address, phone number and bank details.

Urgency

You are made to believe your money is in danger if you don't act immediately.

Phone spoofing

The number of the caller appears as if it is coming from somewhere else so you believe the caller is genuine.

Atmosphere

There is a lot of background noise to sound like a call centre, or they might be playing sound effects.

Holding the line

If you are suspicious, put the caller on hold while you check with your bank. Alternatively, ask for the fraudsters number and tell them you will call them back later.