Information Security Guidelines

Protecting your personal and sensitive information is one of our top priorities.
This awareness guide provides general guidelines on how to safeguard your information, which starts with you, by following best practices both at work and at home.

How to Protect Yourself and Your Information

To protect yourself from fraud attempts or unauthorized access to your data, please follow these instructions:

- **Do not share any personal or financial information** except through the company's official and approved channels, such as:
  - oThe official mobile application
  - oThe official website
  - oVerified phone calls from numbers listed on our website
- If you receive a suspicious call or message, we advise you not to engage, and to contact customer service immediately to verify its authenticity.
- **GATE TO PAY** staff will never ask you for:
  - oYour password
  - oVerification code (OTP)
  - oFull card or bank account details
- If anything feels strange or uncomfortable, end the call immediately and contact us through our official channels to confirm the request.

What is Social Engineering?

Social engineering is a technique used to trick people into revealing personal or confidential information, such as passwords or bank account numbers, without needing to hack any systems.

The scammer pretends to be a trusted entity, such as a company employee or government official, in order to gain the victim's trust and get them to reveal their information.

Common methods include:

- Phone calls
- SMS messages
- Emails
- Social media messages
- Even printed letters or faxes

Important Tip: Never share your personal or confidential information with anyone unless you are certain of their identity, and always use the official channels .

What is Email Spoofing?

Email spoofing is a method used by scammers to send emails that appear to come from a trusted source, while in reality, they are from a **completely different and unauthorized source.**

The goal is to gain your trust and convince you to take a specific action, such as transferring money or revealing sensitive information.

Example: You might receive an email that looks exactly like one you usually get from a trusted party, asking you to transfer money to a new account. In reality, the email is from a scammer and not the real organization.

Important Tip: Always verify the email address carefully and never take financial action or share information unless you're sure the message came from a legitimate, known entity via the official channels.

+962 (6) 200 4717
info@gatetopay.com
www.gatetopay.com
King Hussein Business Park - Building No. 23

Phishing and Fraud Attacks

Phishing attacks are a form of social engineering where scammers trick you into revealing personal information like:

- Credit card numbers
- Passwords
- Bank account details
- Other sensitive data

They usually send fake emails or messages that look like they're from trusted entities, such as a bank or a known company. These messages often contain links to fake websites that are designed to look like the real thing.

Common phishing methods include:

- Emails
- SMS messages
- Phone calls
- Social media messages

Important Tip: Do not click on any link or share your information unless you have verified the source of the message. Be especially cautious with messages that suddenly ask you to update or verify your account details.

For better security, always communicate with gate to pay through our **official channels only.**

Additional Tips to Protect Your Personal Information

- **Only enter your personal or payment information on trusted, secure websites.**
  Always make sure the site shows a lock symbol (□) in the address bar and begins with https://
- **Keep your software and apps updated regularly, especially:**
  - oOperating systems on computers and mobile phones
  - oBanking applications
  - oAntivirus software
- **Make sure you have updated antivirus protection installed.**
- **Shut down your devices when not in use to reduce the risk of unauthorized access.**
- **Do not install apps from unknown or untrusted sources.**

Creating and Using Strong Passwords

Strong passwords are your first line of defense in protecting your accounts. Make sure your password:

- Is at least 8 characters long
- Includes both uppercase and lowercase letters
- Contains numbers and special characters
- Does not include easily guessed info like your name or birthdate
- Is not reused across multiple accounts
- Is never shared with anyone

+962 (6) 200 4717
info@gatetopay.com
www.gatetopay.com
King Hussein Business Park - Building No. 23