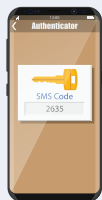# Internet Banking Fraud

Internet banking fraud is a fraud using the Internet or mobile phone technologies to illegally remove money from your bank account and / or transfer money to an account that does not belong to you.
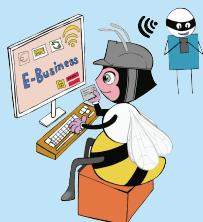
Ensure that your bank provides you with a two-tier authentication mechanism – a 'token' gadget which creates a unique code.

Make sure that your password is eight or more characters and combines letters, numerals and symbols.
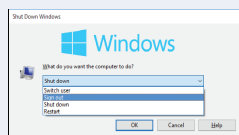
Access your accounts from a secure location, using computers and networks you know are safe and secure. Avoid using public networks.
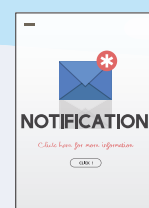
Always look for the padlock icon in the corner of the browser, signalling that the website is encrypted.
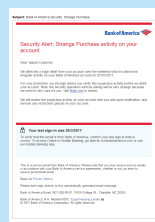
Always sign out and clear your computer's cache at the end of each session.

Set up account notifications to immediately alert you if there is any suspicious activity on the account.

Never respond to urgent emails claiming to be from a bank or any company that requests your account information or personal details.

Post less information on social networking sites. The more information you post, the easier it may be for a criminal to use your information.

Be cautious about messages you receive on social networking sites that contain links. If you are suspicious, do not click the link.

Keep your computer operating system and browser up-to-date with the latest software and security downloads.
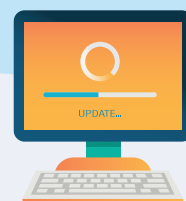
Do not open attachments or install free software from unknown sources; this may expose your computer and the information on it to unauthorised sources.

Install a firewall, antivirus, anti-spyware software package on your computer. These software will detect and remove viruses and spyware.

SCAMS & FRAUDS

ĠEMMA
know, plan, act.

eSkills
eSkills Malta Foundation