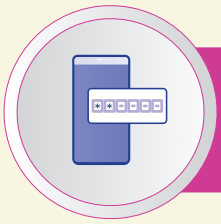
Mobile Phone Scams

With smart phones being so affordable today we use mobile phones not only to communicate amongst ourselves but also to bank, shop, invest, and play skill games, amongst others. Take note of the following tips so that you protect yourself:

If you use your app to carry out Internet banking, use only your bank's official app.

Download apps only from official stores such as Apple iTunes and Android Marketplace.

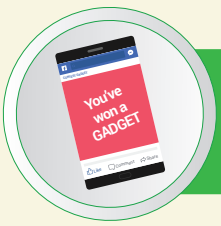
When the phone informs you that you have a new release of your phone's operating system, install this release.



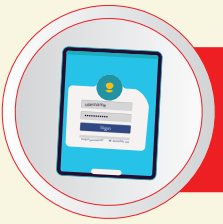
Lock your mobile by a secure PIN number or password which you should not share with anybody else.

There are anti-virus software tools for a mobile – use them insofar as these are from a reputable brand.

Never click links contained on a text or email unless you are sure of the identity of the sender.



You may receive an SMS saying that you have won a great prize – scammers make money by charging high rates for SMSs received from you. Do not reply. If the SMS asks you to call a number to claim your prize do not phone that number.



'Smishing' occurs when a scammer asks for your personal information. Do not reply back. No legitimate business will ask you to provide personal information over the phone.

eSkills
eSkills Malta Foundation

ĠEMMA
know, plan, act.

/ESkillsMalta

@eSkills_Malta

www eskills.org.mt

Scams & Frauds

ĠEMMA
know, plan, act.

eSkills
eSkills Malta Foundation