An Garda Síochána

Campus Watch Information Sheet

Cyber Crime

CW 17

Social Networks

Mobile devices are in everyday use with most students accessing social networking, email, music and information on goods or services, or just sharing information with each other. Recent studies show that 90% of people aged 16-24 use social media while 71% of children using smartphone had increased their usage during the past 18months.

There are many different types of social networking sites. The popularity of each of these sites will change over time depending on tastes. Increased online engagement has seen the number of victims of online abuse continue to rise, with almost 30% of users being victims of online bullying and exploitation. It is important users of online applications are aware of the risks involved as well as the benefits. No platform is entirely secure or safe. By applying the following tips, you can reduce exposure to abusers, hackers, fraudsters, identity thieves and other forms of exploitation.

Popular Online Tips:

Sharing online

- The internet is permanent. Once you post something, even if you delete your account, assume that it is there forever.
- Remember that the control of your photos is no longer yours once you share them online. Never post or share personal or sexual images.
- When accepting a friend, ask yourself - Do you really know them? Only "friend" people you know in the real world.
- Don't trust unsolicited messages. Hackers can break into accounts and send messages that look like they're from your friends. This includes invitations to join new social networks. If you suspect that a message is fraudulent, use an alternate method to contact your friend to verify.
- Manage your privacy settings. Make sure that you are only sharing information with friends and family.
- Turn off the location setting on your smartphone camera. If you plan to share images online, doing this will keep your exact location private.

Content and design by the Garda National Community Policing Unit and the Garda National Crime Prevention Unit.

Cyber Crime

An Garda Síochána

Online Security

- Change your passwords frequently. Choose hard-to-guess passwords which are at least eight characters long with a combination of letters, numbers, and symbols.
- If you have more than one social networking account, ensure that you use different passwords for each one.
- Many social networking sites allow you to download third-party applications that let you do more with your personal page. Criminals sometimes use these applications to steal your personal information. To download and use third-party applications safely, take the same safety precautions that you take with any other program or file you download from the web.
- Your bank won't ask you to verify your account or unlock your account details via an email.
- If you didn't purchase a ticket for the lottery that you 'won', don't respond to the email telling you congratulations.
- Don't respond to messages from friends claiming they have been robbed abroad and need financial help. Contact them first before sending money and never send via a money transfer agency.
- Keep your antivirus protection up to date and be careful what you access to prevent malware/ransomware being downloaded to your system.

Wifi / Links

- Public Wi-Fi can be vulnerable to interception or abuse. Users should take care not to access personal accounts such as social media or bank accounts when using open Wi-Fi networks.
- Don't share passwords and don't save passwords on your computer or when asked to by online profiles or accounts. These can be vulnerable to interception and misuse.
- Only use official websites for services such as Revenue, Sky, Eir or another provider. Don't click on links telling you that you are owed money or that your service will be interrupted if you don't act quickly. Hovering over the link will tell you if it will bring you to where it says it does.

Scams

- Romance Scams are becoming increasingly prevalent. Only join legitimate sites and never offer to financially help potential suitors with travel, business ideas or with a family member'smedical bills. These are likely attempts to defraud you.
- Ignore calls from people telling you they are from software companies such as 'Microsoft'and that they can help you fix your computer. These scams are only interested in your money. If your computer isn't working properly bring it to a repair service or back to the place you bought it.

Campus Watch
Supported by An Garda Síochána

Campus Watch is similar to a residential Neighbourhood Watch scheme in that it is a crime prevention and community safety programme. It operates as a partnership between An Garda Síochána and the campus occupants. It works on the basis that every member of campus can help to improve the quality of life on site by keeping a look out for students, staff and visitors, and reporting suspicious activities to the gardaí.

www.garda.ie

Garda Emergency – 999/112
Garda Confidential Line (Free Phone) – 1800 666111