ProtectUK

IT security and online communications

ProtectUK publication date

06/10/2022

IT security helps to protect the internet enabled devices (smartphone, laptops, PCs) we all use and the services that we access both online and at work from theft or damage.

- use a firewall and anti-virus software and keep them up to date. Run system scans regularly
- be cautious when using third party applications. Malicious codes known as ‘malware’ can spread rapidly around social networks or via email
- do not open emails from unknown or suspicious senders
- treat all email attachments and links with caution. Where it exists, turn off the option to automatically download attachments to emails
- use software controls that ensure only reputable websites can be accessed, reducing the risk of malicious software being installed onto your system
- make sure that the latest updates to your device’s operating system are promptly installed
- check the security protection of your home and business Wi-Fi networks. Change the default (manufacturer) passcode
- do not rename Wi-Fi using identifying details such as your family name
- use a hard-to-guess password and never write it down. Do not tell anyone your password
- do not use the same password for all security log-on purposes
- shred CDs/DVDs before disposal if they contain sensitive information

For further information:

6 ways to Improve Online Security

www.ncsc.gov.uk/section/about-ncsc/what-is-cyber-security

Online Social Networking (OSN)

The internet can be a valuable source of information, education and entertainment for all the family. However, you need to take precautions when using it, especially for social networking purposes.

Internet-based social networking sites such as Facebook, Twitter, LinkedIn and lnstagram are popular applications that allow individuals to create a profile containing personal information and interact with other users. Review your privacy settings to prevent some or all of your OSN profiles being seen by a large audience.

Business networking sites such as LinkedIn also require personal profiles to be created, which normally include an individual's work history.

Whilst these applications are useful tools to communicate with others or advertise professional skills, publishing personal information on your OSN profiles presents potential risks:

- You may be susceptible to identity theft, as dates of birth, full names, home addresses and email details are key pieces of information for identity fraudsters. Some sites 'own' any data posted on them and may reserve the right to sell your details to third parties
- Posting information can put your personal safety at risk. If you provide too much information and do not have the appropriate privacy settings applied, your business or social network accounts can be a veritable 'gold mine' for those intent on building up a picture of your relationships, opinions, places of interest and any other subject that they may seek to exploit in the future
- Location-based information can be posted on social networks, especially from GPSenabled mobile devices, which tells others exactly where you are or have been. This information is not secure and could be viewed by anyone, including those who may want to harm you or your family, friends and colleagues. The responsibility rests with you to ensure that no-one is put at

risk due to what is disclosed

- Regularly check what information you can find out about yourself, your family or your business on-line and edit where able

You should not include personal details such as:

- mobile phone numbers
- personal or work addresses
- employment details
- level of security clearance
- family members
- hobbies and places frequented
- vehicle details
- work information on personal accounts

To avoid putting other people at risk, photographs of family, friends and colleagues should only be published with your consent and theirs.

If applicable, published photographs should not reveal your occupation, home or place of work. Review your account settings.

Disable photo and location tagging, so you have to approve another user identifying you in a photograph or being at a specific location. Ensure your privacy settings are adequate and your account is as locked down as it can be.

It is equally important that family and friends are made aware of any risk, in order for them to take suitable precautions with their online presence. This is especially relevant if they are used to posting content about the person ‘at risk’.

For further information

ProtectUK app

The publicly available ProtectUK app is designed to help the public spot the signs of suspicious behaviour and understand what to do in the event of a major event.

The app contains live-time information from Counter Terrorism Policing and protect security advice.

Powered by Urim, the ProtectUK app is free for members of the public and businesses and has been developed in partnership with industry specialists from Marks and Spencer and Highfield e-Learning. Available from Google Play or App Store, the app will provide access to:

- practical advice and guidance to help you protect your business, plus information on how to respond in the event of an attack
- information on Counter Terrorism Policing's suite of ACT training products, plus access to the online e-Learning package
- suite of National Counter Terrorism Security Office guidance videos
- latest reference documents and publications
- ACT online reporting and anti-terrorist hotline
- emergency Response and post incident guidance
- live-time news updates from UK Protect

Further links

https://www.npsa.gov.uk/security-campaign-assets/digital-footprint-2017

www.ncsc.gov.uk/section/information-for/individuals-families

CHILDREN'S PERSONAL SAFETY ONLINE

Information and support for young people/parents and professionals is available at:
www.thinkuknow.co.uk
Child Exploitation and Online Protection Centre (CEOP): www.ceop.police.uk