Web Links

Cybercrime: C**riminals** exploit the speed, convenience and anonymity of the **Internet** to commit a range of **criminal** activities. These know no borders, either physical or virtual, can cause serious harm and pose very real threats to victims worldwide. **Cybersecurity** is the planned defence against Cybercrime. These free web-links may be useful follow-up to tonight's discussion, and for folk who were unable to join with us. Thanks is given to those organisations that make this information freely available:

* **Cyber Crime and Why it matters ……..**

http://www.media.barclays.co.uk/serve/176668-5610838.mp4

a 4 minute presentation for small businesses from Barclays Bank.

*** Being aware of "social engineering"**

http://www.media.barclays.co.uk/serve/176669-2585621.mp4

a 7 minute presentation for small businesses from Barclays Bank.

*** Common cyber threats – what to look out for …….**

http://www.media.barclays.co.uk/serve/176670-5417778.mp4

a 7 minute presentation for small businesses from Barclays Bank.

*** Protect yourself ……**

http://www.media.barclays.co.uk/serve/176671-3619165.mp4

remain safe online, using malware protection and managing who needs access to what. A 6 minute presentation from Barclays Bank.

*** National Crime Agency** – an extensive website with useful free follow-up material:

http://www.nationalcrimeagency.gov.uk/crime-threats/cyber-crime

Some tips to help protect against cyber criminality:

1. Use a full-service internet security suite

e.g., *Norton Security* provides real-time protection against existing and emerging malware including ransomware and viruses, and helps protect your private and financial information when you go online.

2. Use strong passwords

Don't repeat your passwords on different sites, and change your passwords regularly. Make them complex. That means using a combination of at least 10 letters, numbers, and symbols. A password management application can help you to keep your passwords locked down.

3. Keep software updated

This is especially important with your operating systems and internet security software. Cybercriminals frequently use known exploits, or flaws, in your software to gain access to your system. Patching those exploits and flaws can make it less likely that you'll become a cybercrime target.

4. Manage social media settings

Keep your personal and private information locked down. Social engineering cybercriminals can often get your personal information with just a few data points, so the less you share publicly, the better. For instance, if you post your pet's name or reveal your mother's maiden name, you might expose the answers to two common security questions.

5. Strengthen your home network

It's a good idea to start with a strong encryption password as well as a virtual private network. A VPN will encrypt all traffic leaving your devices until it arrives at its destination. If cybercriminals do manage to hack your communication line, they won't intercept anything but encrypted data. It's a good idea to use a VPN whenever you a public Wi-Fi network, whether it's in a library, café, hotel, or airport.

6. Talk to your children about the internet

Teach your kids about acceptable use of the internet without shutting down communication channels. Make sure they know that they can come to you if they're experiencing any kind of online harassment, stalking, or bullying.

7. Keep up to date on major security breaches

If you do business with a merchant or have an account on a website that's been impacted by a security breach, find out what information the hackers accessed and change your password immediately.

8. Take measures to help protect yourself against identity theft

Identity theft occurs when someone wrongfully obtains your personal data in a way that involves fraud or deception, typically for economic gain. How? You might be tricked into giving personal information over the internet, for instance, or a thief might steal your mail to access account information. That's why it's important to guard your personal data. A VPN — short for virtual private network — can also help to protect the data you send and receive online, especially when accessing the internet on public Wi-Fi.

9. Know that identity theft can happen anywhere

It's smart to know how to protect your identity even when travelling. There are a lot of things you can do to help keep criminals from getting your private information on the road. These include keeping your travel plans off social media and being using a VPN when accessing the internet over your hotel's Wi-Fi network.