Knowledge Transfer Network
ICT

Technology Strategy Board
Driving Innovation

Cybersecurity – Simple Tips

- For any business – produce a documented Risk Assessment. Consult with an expert to help you identify the risks and threats. This enables *prioritisation* of your resources to achieve an *appropriate* level of protection *tailored* to your business. It imparts structure to your methods and enables continuous and measured improvement. See www.iasme.co.uk for help.

- If your business hosts a website or is heavily reliant on web sales or Internet facing connectivity, consider using a secure interface such as SSL (identified by a small padlock next to the address). Consider having an annual penetration test ('pentest') to check your technical configuration for weaknesses. It's the only way to really know what opportunities you are giving an attacker.

- Enable and use the built-in security functions of your hardware and software. Sadly these are often disabled by default. Your router is likely to have a firewall built in – enable it. Windows and Apple operating systems also have a built in firewall which should be enabled.

- Use an Anti-Virus app and update it regularly – at least once a day. With any good app this can be done automatically. For non-commercial use there are several good free AV products, but for commercial use be prepared to pay a little. You get what you pay for, and most paid applications also offer additional security measures.

- Many compromises occur as a result of a user opening an infected email attachment or following a "bad" link and getting an uninvited visitor. Don't open email attachments unless they're from someone you know or they are expected. If in doubt, virus check them before opening. Don't just click on links to follow them – copy and paste them into your browser URL field and then check them. NEVER trust emails bearing links to well-known providers/banks… go to the site by using your normal Bookmark or method rather than following a link in an email.

- "Shoulder surfing" (watching what someone types over their shoulder from behind) remains an easy and popular way to get your passwords – be aware! If a stranger can see your screens there are simple screen stick-on products which can restrict viewing angles.

- Try not to use open WiFi networks in Shopping Centres and Coffee Shops unless you use a VPN (a secure tunnel for your communications) – they're ideal venues for attackers to sit and gather your information. If you do, do not visit sites that require you to enter your password. There are free or cheap products which offer a temporary VPN for just such circumstances.

- If your website is important to your business, ask your hosting provider what they do to protect it. Ensure you have a Service Level Agreement or that the provider has security certification.

Knowledge Transfer Network
ICT

Technology Strategy Board
Driving Innovation

Cybersecurity – Simple Tips

- It's not just attackers who can threaten your business – data loss can occur through hardware failure and mistakes too. Ensure you regularly backup your data… AND that you know how to restore it. Test that you can. It's best to learn any lessons when you're not waist deep in alligators!

- Be careful over what personal information you put online – especially across the range of Social Media sites. It may be easier for an attacker to build up a profile of you and steal your identity than it is to break into your system. They will collect information from many sites to put together a detailed picture of your life, habits, family, employment, hobbies, children, friends, pets, locations etc. Attackers are now inventing false identities on media sites such as Facebook and LinkedIn, so be careful who you make friends with!

- Use strong passwords. Use a rhyme or song to remember them or use one of the many available apps which securely stores them for you and protect access to the app with a single strong password you can remember. Do *NOT* use the same password across multiple sites!

- Watch out for removable media such as USB Memory sticks. Don't allow others to plug them into your system unless you trust the person or virus check the media first. Don't lend your sticks to others and then use them yourself. Remember as soon as you plug them in they can execute malware – so formatting/wiping them as a protective measure can be too late. If you put valuable data on a stick remember to encrypt it – buy sticks with encryption built-in or use one of the free encryption products.

- Turn your machine *OFF* when you're not using it – so that others can't use your credentials.

- If a member of staff leaves your organisation, remove their accounts – asap but definitely *before* they leave site. Don't share passwords or account details with anyone.

- Look here: http://www.iasme.co.uk/index.php/10steps for the 10 Steps recommended by UK Govt. translated into an easier to understand version by IASME. Don't think that you have to implement them all (though great if you can)… choose ones which are good for you. Any improvement is worthwhile!

- Consider IASME if you are a business with a supply chain requiring some assurance from you. It's a great way to demonstrate to customers and suppliers that you take security seriously and are safe to do business with. You can even self-certificate.