BEER MAT MENTORING MEETING NOTES

(14) Information security

The Internet and all that is a wonderful thing. But there's a dark side. There are people all over the world quietly pushing the door to your digital fortune to see if it's locked.

Here are some key considerations. This is not just about your own accounts but your customers' data. The Information Commissioner's Office can impose large fines if you don't keep this secure.

1 Use strong passwords

- "123456", "password", and "qwerty" are still popular passwords; www.dinopass.com has better ones.
- Use a different password for each website. www.dashlane.com or https://lastpass.com will help you remember these passwords.
- Your email address is probably the key to resetting the password for every other website service you use. Secure it with a strong password and look into how to set up two step ("Multi-Factor") authentication.
- Use passwords as the answers to your security questions. Name of your first pet? "h@ppySugar79".

2 Keep your information secure when travelling

- Consider a "MiFi" dongle or "tethering" your smartphone to avoid using unsecured Wi-Fi.
- Don't advertise! A laptop sleeve inside another bag is less obvious than a Targus or HP case.
- At exhibitions, secure your laptop to something solid to stop opportunistic theft.

3 Take backups

- What are you guarding against? The "whoops" factor of deleting a file? Your hard drive crashing? A burglary or fire where you lose your backup drive and laptop? An HMRC audit asking for files from 2012?
- Use a cloud backup service like Mozy or Carbonite to back up all new or changed files. Around £10/month.
- A backup strategy - buy multiple USB flash drives. Each month, back up your key documents, then label it and store somewhere safe, not next to the computer. Try restoring some files.
- Replication (e.g. Dropbox, Google Drive) is useful, ensuring the same document on several devices, but if you delete it on one device, it will (eventually) be deleted everywhere.

4 Turn on security options

- Set your computer to install security patches. Run an antivirus program.
- Other programs have patches too – use https://ninite.com to update Dropbox, Skype etc. in one click.
- Protect your mobile phone with a PIN. Take backups. Turn on the "find my phone" feature. Decide if you want to be able to wipe it automatically / after 10 incorrect attempts at inputting your PIN.
- Consider hard-drive encryption (Windows Bitlocker) which will mean that even if someone steals your PC, they can't get to the information. If you lose the key, you won't be able to get to the information either!

5 Humans are the weakest link!

- If you're not expecting an email with a link or attachment then delete it, or check via your phone.
- Watch out for sophisticated scams where "Microsoft" asks you to install a program or the "RPA" calls about a recent payment.

Further advice is available at https://www.getsafeonline.org/business/ and https://www.cyberstreetwise.com/protect-your-business

NOTES