Keeping your devices and software up to date

Your computer

- Computer operating systems are made up of countless parts with different functions, ideally working in harmony. It's inevitable that some of these parts will be less than perfect. But when a problem leaves a hole in your machine's defenses, it is extremely important to patch it up as soon as possible. This is best accomplished by using built-in and automatic update features. Follow your specific device manufacturer's best practice recommendations, usually found via their main websites.
- Third-party applications all need regular updating. It is very important that you check all of the programs that you use for built-in updating
- g options. It's also a good idea to make sure that you have the most recent version of the software. Checking the vendor's website is typically the best first step.
- Allowing your software, especially browsers and anti-virus software to become out-of-date only gives hackers and fraudsters more opportunity to do damage. By running out-of-date software, you open yourself up to malicious software and viruses which can allow your information to be compromised – with serious consequences, including identify theft and financial loss. Your computer or device may well become unusable, and your data can be permanently lost.

- Anti-virus software is a key component to protecting your computer. Anti-virus software scans files or your computer's memory for certain patterns that may indicate an infection. The people who create viruses are continually releasing new and updated viruses, so it is important that you have the latest definitions installed on your computer.
- Choose a well-known company and simply go to their website, choose a price point and level of security and download according to the instructions.
- Once you have installed an anti-virus package, you should scan your entire computer periodically. You can do this in two ways:
- Automatic scans - Depending what software you choose, you may be able to configure it to automatically scan specific files or directories and prompt you at set intervals to perform complete scans.
- Manual scans - It is also a good idea to manually scan files you receive from outside sources before opening them. This includes:
- Saving and scanning email attachments or web downloads rather than selecting the option to open them directly from the source.
- Scanning media, including memory sticks, CDs and DVDs, for viruses before opening any of the files.

- A lot of times your device will come with protection for a trial period. You can extend this type of protection if it suits you by following the steps given, but it is a good idea to confirm that this is the software that has been provided by the seller.
- Alternatively, you can seek out a service that covers your needs online.
- Here are some links to more information on protecting your computer.

Your mobile device, including phones and tablets

- Keep your device software up-to-date by running the update functionality on a regular basis.
- Set up your device with an access password/passcode.
- Smartphones and tablet devices are just mini fully-fledged computers. You need to take the same precautions with your smart phone or other device that you do with your personal computer when shopping, banking, or sharing personal information online as they are susceptible to risks inherent in online transactions. Because they are portable, you should also take precautions to keep your devices themselves safe.

- Consider the way you are accessing the Internet: Avoid using open Wi-Fi networks to conduct personal business, bank, or shop online. Open Wi-Fi networks at places such as airports, coffee shops, and other public locations present a golden opportunity for attackers to spoof a Wi-Fi router or intercept the sensitive information that you provide to complete your online transaction.
- Bluetooth-enabled accessories such as earpieces for hands-free talking can be helpful. However, they can also be used by attackers to gain access to your device. When these accessories are not in use, turn off the Bluetooth setting on your mobile device. Cyber-criminals have the capability to access your phone's open Bluetooth connection when you are not using it and steal personal information.

If you believe that one of your online accounts has been compromised, you should call whoever your account is with to report the suspected fraud. Ensuring that you do this in a timely manner helps minimize the impact. You should also change your account passwords for any online services associated with your mobile device using a different computer that you control.