Part I - Cyber Security Top Tips

How to create a strong password

It is an usual time and we are depending significantly on technology to connect with friends and family, work remotely at home as well as get the latest news. While ensuring ourselves are healthy both physically and mentally, it is equally important to keep our data safe online.

The UK has seen a surge in cyber crime during the Pandemic, over 1,000 cases of Coronavirus-related fraud and cyber crime were reported in April alone *(National Fraud Intelligence Bureau, Apr)*. Cyber criminals play on the public fears by sending out 'tips' that lure internet users to click on malicious links or files so to steal personal data and identity.

Passwords act as the key to your digital footprint, including your emails, social networks, shopping, online banking and more, leaving you vulnerable to identity theft. The following **DOS** and **DON'TS** checlists help you to build a robust first line of defence to prevent you becoming a victim of cyber crime.

DOS

- ✓ Use a combination of uppercase, lowercase letters, symbols and numbers.
- ✓ Make sure that your passwords are at least eight characters long; the more characters, digits and symbols your password contains the harder it is to guess.
- ✓ Consider using a password made up of a phrase with some characters replaced with symbols and numbers.
  - Example : I like to eat apple pie
  - Becomes : **iL1k3t0e@tapPl3p1e**
- ✓ Log out of websites and devices when you are finished using them.
- ✓ Use multi-factor authentication (MFA) whenever possible.
- ✓ Get a password manager if you need help remembering all your online passwords.

DON'TS

- ✓ Do not use the same passwords for all your devices and websites.
- ✓ Do not use common, easy passwords such as those listed under Common Passwords.
- ☐ Do not use a single word that exists in a dictionary such as **"chocolate"** or **"invincible"**.
- ☐ Do not use any derivative of your name, the name of a family member, loved one or pet.
- ☐ Do not use any phone numbers, addresses, birthdays, significant dates, car registration or your National Insurance number.

PART II - Cyber Security Top Tips

How to protect your smartphones and tablets

During COVID-19, staying connected has been hugely important. One phone provider has reported a **45% increase** in usage as well as a **70% rise** in the use of social media platforms. The statistic below also show how much we rely on our phones and mobile devices. It is essential you know how to follow some good mobile device housekeeping in order to stay secure online.

Smartphones and tablets now make up **52%** of Internet traffic.

65.7% of people sleep with their smartphones at night.

87.8% of people feel uneasy leaving home without their smartphones.

36% of people would go without their smartphones for "one week or less" if it meant that all of their debts were erased.

17.3% of people spend more time on their smartphones than with their children.

PIN LOCK
& DEVICE ERASE

Smartphones support the feature of requiring a PIN in order to access the device, many devices even support biometric locks involving fingerprints and facial recognition. These screen locks are an important extra layer of security if someone got hold of your device. Cyber criminal will not be able to access the data on your device, such as mobile banking and emails, without entering your password, pattern, PIN or fingerprint.

Especially when smartphones also support a feature where the device will be wiped if the incorrect PIN is entered a set number of times. It is essential that your mobile device is secured by at the very least a PIN and preferably also by some form of biometric security.

Recap - how to create a strong password

- Use a combination of uppercase, lowercase letters, symbols and numbers.
- Do not use the same passwords for all your devices and websites.
- Do not use any phone numbers, birthdays, car registration or your National Insurance number.
- Don't use '1,2,3,4' or an 'L' shaped pattern which are easy for other people to guess.

PART II - Cyber Security Top Tips

How to protect your smartphones and tablets

OPERATING SYSTEM & APP UPDATES

All modern smartphones support software updates for both the underlying operating system as well as any Apps that you use. On most devices updates can be applied automatically from the App Store (iOS) or the Play Store (Android).

FIND MY DEVICE

Smartphones and tablets are equipped with a feature enabling you to track the location of your device.

- Android : Find My Device
- iOS : Find my iPhone

Using this feature enable you to track the last known position of your smartphone in the event of loss or theft. It is also possible to lock or erase data on the device remotely using these services. It is highly recommended that you activate this service on your smartphone and devices.

PUBLIC WI-FI NETWORKS – HAVE YOU HEARD OF "THE STARBUCKS SCAM"?

It is a public Wi-Fi scam, using Starbucks as an example. These free public Wi-Fi are often used by cyber criminals to tempt you to connect to the Wi-Fi in order to steal your personal information. Only ever connect your devices to known, trusted Wi-Fi networks. If possible, use your 4G/5G connection instead.

You enter a coffee shop and set down with your coffee

You decide to connect to a public Wi-Fi and see a "Starbucks Free Wi-Fi"

So, you connect and start browsing the Web

Meanwhile, the cyber criminal who is operating the Wi-Fi point you connected now have access to your device and data, e.g. passwords, photos and emails.

Part III - Cyber Security Top Tips

How to conduct a video conference safely

Video Conferencing (VC) is an effective tool to support communication when meetings cannot take place face to face. It is especially demanding when a lot of us are working from home now. In line with Data Protection Policies, you should ensure to have systems and procedures that allow video conferencing to be set up and used safely. This time, we are going to discuss how to conduct a video conference securely.

Before you start

1. Agree which video platform will be used within the business. Software such as ZOOM, Microsoft Teams and Skype for Business are intended for business use.
2. Read the Terms and Condition of the licence to make sure you understand the privacy settings.
3. Ensure your Operating Systems are up to date including virus checking software.
4. Ensure that the latest software version of the video conferencing tool is downloaded.

Setting up a meeting

1. When setting up a VC, send the link to a meeting in an email to individuals. Do not post it on social media.
2. Personalised setting on your VC platforms, e.g. set up the meeting so that participants are muted when they join initially or only the host can share their screen unless approved.
3. If you wish to record the meeting, make sure you have got everyone's consent.
4. Make sure you verify the participants if you using audio function only.
5. Where the virtual waiting area is available, use this to verify participants who are outside your organisation or who are unknown to you prior to the conference.

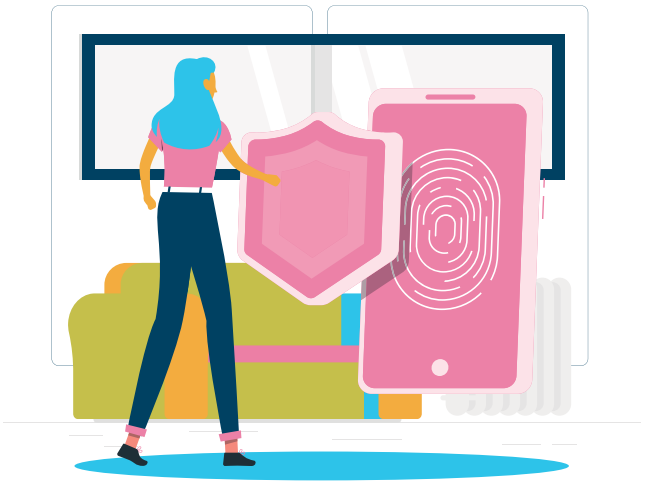
Attending a Video Conferencing meeting

1. Treat the VC like you would a face to face meeting.
2. Before the meeting begins, check that your video conferencing equipment works, such as the headphones. You should know when your webcam and microphone are activated.
3. Consider blurring the background to protect your privacy.
4. Mute your sound when you are not speaking but remember to unmute to speak.
5. Knowing when to speak can be difficult when there are multiple participants, consider raising you hand if you wish to speak.
6. Try to avoid multi-tasking during a VC, as other participants might see it.
7. Hold accountable for what you say, even it is a virtual meeting.
8. Some VC software allows private messaging. Be aware that the host can still see this in a transcript at the end of the call.
9. If discussing something private or confidential, make sure you are somewhere the discussion cannot be overheard.

Part IV - Cyber Aware Top Tips

How to browse the web safely and avoid email scam

COVID-19 has meant that we must work differently, whether its registering on the capacity tracker or searching for PPE from suppliers. But even if you are internet savvy, there are cyber attackers looking to take advantage of those that are unprepared and find different ways to exploit care providers that are busy taking care of service users. In the last part of the series, this fact sheet will give you some tips on safe web browsing and how to identify an email scam.



SAFE WEB BROWSING

In general, modern websites should all use an encrypted connection which you will be able to verify based on the website address (otherwise known as the URL).

- An encrypted connection:
  https://www.securesite.com/
- No Data Encryption Implemented:
  http://www.unsecuresite.com/

The leading **https** denotes an encrypted connection, meaning that the data sent between your computer and the website is encrypted and cannot be intercepted or changed by third parties. When connecting to a secure website your browser address bar will show a padlock icon.

BE CAREFUL
WITH DOWNLOADS

Only download files from trusted sites and be very careful about running any executable or installable applications that you have downloaded. Ensure that you are especially careful when downloading free software to ensure that it does not contain malware. Always make sure that you perform a virus and malware scan with your chosen anti-malware software before opening the downloaded files. Make sure you have the most up to date version of any anti malware software too!

Part IV - Cyber Aware Top Tips

Safe Web Browsing and Email for Social Care Providers

SAFE EMAIL USE

More than 91% of successful cyber attacks start from an email. Typically, these emails will include either one or more attachments, or they will entice you to click on a link. Modern emails of this nature have become increasingly sophisticated and some can be very difficult to detect.

HOW TO DETECT A FRAUDULENT EMAIL?

1 Check the sender's email address

Hover your mouse over the sender's name and you should be able to assess an actual and a fraudulent emails addresses:

- The email might show this:
  accounts@barclays.com
- Hover your mouse, and you might see this instead:
  scan_ro1561@lix.ru

2 Check the link

If you are ever in any doubt, do not click any links in emails. Similar to checking the email address:

- An email may show:
  https://www.barclays.com/accounts
- Yet, when hovered over the link may show:
  http://sxdc.ru/?rf=136403204bbd

You can also determine the reliability of the link by typing the actual address on a web browser.

3 Look for errors

Cyber criminals often demonstrate poor English skills. Keep a close eye for the following:

- Spelling mistakes e.g. **"Aeroplane" vs "Airplane"**
- Grammatical mistakes
- Punctuation mistake
- Non-English spelling, phrases or colloquialisms

4 Check the link

If you have any doubts, treat all email as suspicious until proven otherwise and apply your common sense. You can't win money or a prize in a lottery you haven't entered.