Are you staying alert?

Social media is a great way of keeping in contact with family and friends but it is wise to consider exactly what you share online and to be mindful of how that information could compromise you and your family's safety.

Police digital crime units regularly deal with victims who have fallen foul of cyber criminals due to the unwitting release of personal information about themselves and others.

However, we can all do some simple things to increase our safety. Here are some tips for you to follow:

- Google yourself to find out where you appear online - past posts or records will still exist and you can request they're removed
- Review your security settings across all platforms and set them to the highest level. Do this regularly, especially after any app updates as they can revert back to default settings
- Consider if what you're sharing on personal online accounts could identify details about you, your family or where you live. It's advised not to include your address and date of birth
- Discuss with your family and friends what they're sharing about you and their security settings as they may be giving personal details about you
- Be selective with requests to connect with you on all social media platforms. If you don't know the person don't accept them. It could be a fake account
- Think about removing your details from the open electoral register and sites that supply that information such as 192.com, Yell.com and White Pages
- Don't set up personal online accounts using your work email address
- Be careful what you're sharing about police buildings or colleagues online
- Never compromise operational security on social media
- To prevent someone tracking your movements and identifying your home or place of work, it is important to limit or disable location services – turn off WiFi and Bluetooth when you don't need them
- Consider having a username on your personal accounts which doesn't immediately identify you, i.e. use first and middle name rather than surname - Elizabeth Jane
- Have a strong password, for example, made up of three random words
- It's your responsibility to keep your personal details safe online
- If you're concerned the safety of your personal online accounts has been compromised in any way contact your local police and inform your line manager
- For more tips and advice visit staystafeonline.org.

Data Protection

Europe is now covered by the world's strongest data protection rules. The mutually agreed General Data Protection Regulation (GDPR) came into force on May 25, 2018, and was designed to modernise laws that protect the personal information of individuals.

Before GDPR started to be enforced, the previous data protection rules across Europe were first created during the 1990s and had struggled to keep pace with rapid technological changes. GDPR alters how businesses and public sector organisations can handle the information of their customers. It also boosts the rights of individuals and gives them more control over their information.

Elizabeth Denham, the UK's information commissioner, who is in charge of data protection enforcement, says GDPR brings in big changes but has warned they don't change everything. "The GDPR is a step change for data protection," she says. "It's still an evolution, not a revolution". For businesses which were already complying with pre-GDPR rules the new should be a "step change," Denham says.

But there has been plenty of confusion around GDPR. To help clear things up, here's WIRED's guide to GDPR.

The GDPR is Europe's new framework for data protection laws – it replaces the previous 1995 data protection directive. Previous UK law was based upon this directive.

The EU's GDPR website says the legislation is designed to "harmonise" data privacy laws across Europe as well as give greater protection and rights to individuals. Within the GDPR there are large changes for the public as well as businesses and bodies that handle personal information, which we'll explain in more detail later.

After more than four years of discussion and negotiation, GDPR was adopted by both the European Parliament and the European Council in April 2016. The underpinning regulation and directive were published at the end of that month.

After publication of GDPR in the EU Official Journal in May 2016, it will come into force on May 25, 2018. The two year preparation period has given businesses and public bodies covered by the regulation to prepare for the changes.

GDPR applies across the entirety of Europe but each individual country has the ability to make its own small changes. In the UK, the government has created a new Data Protection Act (2018) which replaces the 1998 Data Protection Act.

The new UK Data Protection Act was passed just before GDPR came into force, after spending several months in draft formats and passing its way through the House of Commons and House of Lords. The Data Protection Act 2018 can be found here: http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted.

As the law was passed there were some controversies. It was amended to protect cybersecurity researchers who work to uncover abuses of personal data, after critics said the law could see their research be criminalised. Politicians also attempted to say there should be a second Leveson inquiry into press standards in the UK but this was dropped at the last minute.

As well putting new obligations on the companies and organisations collecting personal data, the GDPR also gives individuals a lot more power to access the information that's held about them.

A Subject Access Request (SAR) allows an individual the ability to ask a company or organisation to provide data about them. Previously, these requests cost £10 but GDPR scraps the cost and makes it free to ask for your information. When someone makes a SAR businesses must stump up the information within one month. Everyone will have the right to get confirmation that an organisation has information about them, access to this information and any other supplementary information. As Dixon points out, big technology companies, as well as smaller start-ups, will have to give users more control over their data.

As well as this the GDPR bolsters a person's rights around automated processing of data. The ICO says individuals "have the right not to be subject to a decision" if it is automatic and it produces a significant effect on a person. There are certain exceptions but generally people must be provided with an explanation of a decision made about them.

The regulation also gives individuals the power to get their personal data erased in some circumstances. This includes where it is no longer necessary for the purpose it was collected, if consent is withdrawn, there's no legitimate interest, and if it was unlawfully processed.