Key Points

Throughout the workshop we repeat a few key ways a victim's accounts and devices can be protected to reduce the impact of any malpractice.

Many of the crimes reported can be avoided by following a small set of tips; we will be reiterating these during the session.

Do not reuse passwords

If you reuse passwords across accounts, once someone has access to one account they may be able to access many more. For most people, the most common threat is that one of their accounts is compromised in a data breach; for the victim of crime their abuser may have found out a password from one account and been able to use it elsewhere.

Ideally no two accounts should have the same password, but this can be hard to put into practice. The NCSC supports the use of password managers, saving to the browser, or writing down passwords and keeping them in a safe place, as these options make it easier to use unique passwords. However all should be used with caution in a domestic abuse situation, as the abuser might be able to access the passwords. It may be better to commit a small number of strong passwords to memory for the most critical accounts.

Some accounts are more important than others, such as email, bank or phone-related ones (e.g. iCloud or Google) and should be prioritised with unique, strong passwords. One of the most important accounts is email, as it can be used to reset the password for almost all other accounts - if you select 'forgot password' on most sites and accounts, a reset link will be sent the the email account used to register the account. If an abuser has access to email, they will be able to reset and access almost all other accounts.

Passwords should not be:

Easy to guess because they are commonly used, e.g. passw0rd

Easy to guess by someone who knows you well, e.g. your pet's name

Easy to crack because they are technically weak, e.g. a single dictionary word

For most people, commonly used and weak passwords are the greatest threat as they are most likely to fall victim to untargeted, brute force attacks. For the victim of abuse, personal passwords can be more of a problem, as the attacker is someone who will know them well enough to guess those passwords.

The NCSC guidance recommends using three random words to produce sufficiently strong passwords. You can add a mix of upper case, lower case, numbers and special characters, especially if the site or app demands these things.

Do not share accounts

If you share an account, either because it's a joint account such as a 'couples' Facebook profile, or because you have given the login details to someone else, this can give free access to your photos, videos, emails, money, contacts, etc. An abuser will be able to able to delete, steal, share or manipulate all these things.

If login details have been shared willingly with an abuser it will make it much more difficult to prove a case against them.

Two step verification/two factor authentication

Two step verification (2SV) or two factor authentication (2FA) are ways to add extra protection to accounts. Both mean that something extra is needed, in addition to username and password, to get into an account. This is commonly an SMS sent to your phone (which means only the person holding the phone can access the account) but can be other methods.

2SV/2FA can:

Alert you to attempts to access the account

Prevent certain activities happening, e.g. payments being made.

Help to build evidence against an abuser

Never share the codes sent as part of 2FA/2SV with anyone else as this will allow abusers access into your accounts.

Backups and software updates

Keep your devices as up to date as possible. If devices are fully up to date it will mean that known flaws are fixed, and cannot be exploited to harm you.

Older devices cannot always be kept fully up to date. They should be kept as up to date as possible. Other tips explained in these guides will help keep you safe, even if there are unfixed flaws in your device.

Backing up your photos, videos, files etc means that you will be able to get them back relatively easily if you lose access on your device, for instance if it is stolen. See App Protection & Settings for possible risks if you share a backup destination (e.g. iCloud) with an abuser.