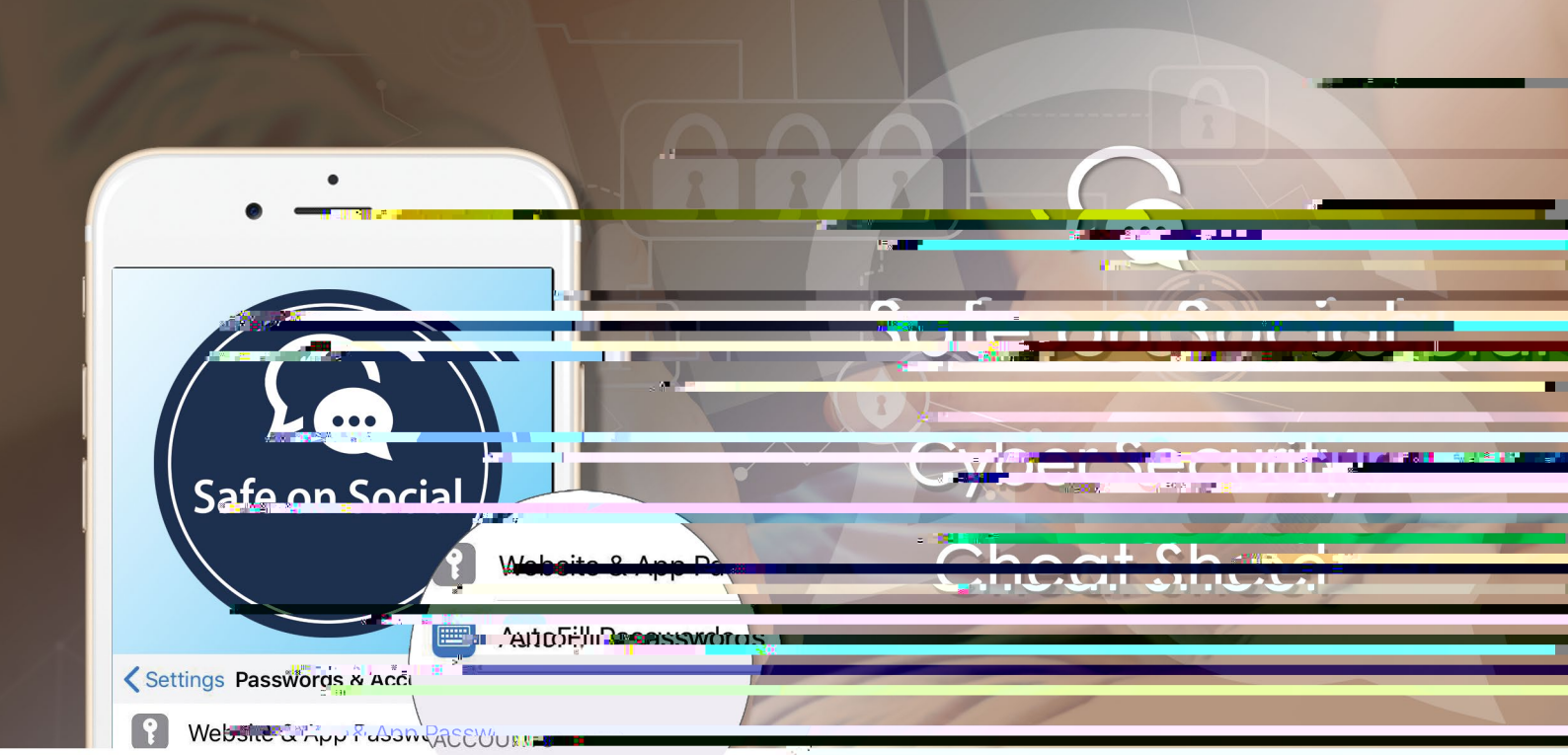

C be Sec

Don't ever think "It won't happen to me". Everyone, on every device that is connected to the internet, is at risk of being hacked, succumbing to a virus, being a victim of a phishing scam, malware, ransomware and other attacks are also rife.

Your personal and financial well-being through to your professional reputation and everything in between can be at risk, so we all need to continue to take Cyber Security seriously.

At Safe on Social, we believe that learning good Cyber Security practices should underpin everything that we do online.

Pa d a a e e

Use long passwords 20 characters or more are best.

Use a healthy mix of characters, preferably alphanumeric, and never use the same password for multiple sites because if a hacker can access one of your accounts, it will only be a matter of time before they have your whole online life at their fingertips.

Always use a password/passcode or biometric to lock your mobile device that way if it is lost or stolen, people won't be just a pin code away from access your bank account, your social media account and many other personal things like photos.

As hard as it may seem, please don't share your passwords and don't write them down.

Update your passwords periodically, at least once every six months (90 days is better).

If you are an an Apple user, consider using the free Keychain Access to manage passwords.
Keychain Access is a macOS app that stores your passwords and accounts information and reduces the number of passwords you have to remember and manage.

When you access a website, email account, network server or another password-protected item, you may be given the option to remember or save the password. If you choose to keep the password, it's saved in your keychain, so you don't have to remember or type your password every time.

To ensure that passwords and other data stored in your keychain are secure, make sure to set up a login password for your computer.

Alternatives to Keychain Access for Windows, Mac, Android, iPhone, Linux and more can be found in this article just released by CNet, The article outlines the best password managers should you want to invest in one. https://www.cnet.com/news/the-best-password-managers-directory/

A password manager can help you to maintain strong, unique passwords for all of your accounts. These programs can generate strong passwords for you, enter credentials automatically, and remind you to update

Kee a de ce f, a e , da, e

Installing software updates for your operating system, apps and programs when prhe

Ne e ea e de ce a e ded

The physical security of your device is just as important as its technical security.

If you need to leave your laptop, phone, or tablet for any length of time password lock it so no one else can use it.

If you keep sensitive information on a USB Flash Drive or external hard drive, make sure to keep them password locked as well.

For desktop computers shut-down the system when not in use or lock your screen. If you are using a device in a library or hotel foyer etc. – don't forget to log out!

P ec e e da a

Be aware of sensitive data that you come into contact with.

Keep sensitive data (e.g student records, health information, etc.) from being saved to your device. Keep it off of your workstation, laptop, or mobile devices.

Securely remove sensitive data files from your system when they are no longer needed.

Always use encryption when storing sensitive data.

U e b e de ce afe

Considering how much we rely on our mobile devices, seriously consider implementing all of the following.

Lock your device with a PIN, password or a biometric (fingerprint or facial recognition).

Only install apps from trusted sources.

Keep your device's operating system updated.

Don't click on links or attachments from unsolicited emails or texts.

Re a bac. da a

Most devices are capable of employing data encryption through two-factor authentication consult your device's documentation for available options.

Use Apple's Find my iPhone
https://www.apple.com/icloud/find-my-iphone/

alternatively, the Android Device Manager
https://support.google.com/accounts/answer/6160491?hl=en

Back up on a regular basis - if you are a victim of a security breach, the only guaranteed way to repair your computer is to erase and re-install the system.

I a a - ec

Only install an anti-virus program from a known and trusted source. Keep device software up to date to ensure your anti-virus program remains effective.

w: safeonsocial.com
e: wecanhelp@safeonsocial.com