



Keeping data secure

DATA SECURITY



General Principles: Keeping data secure online

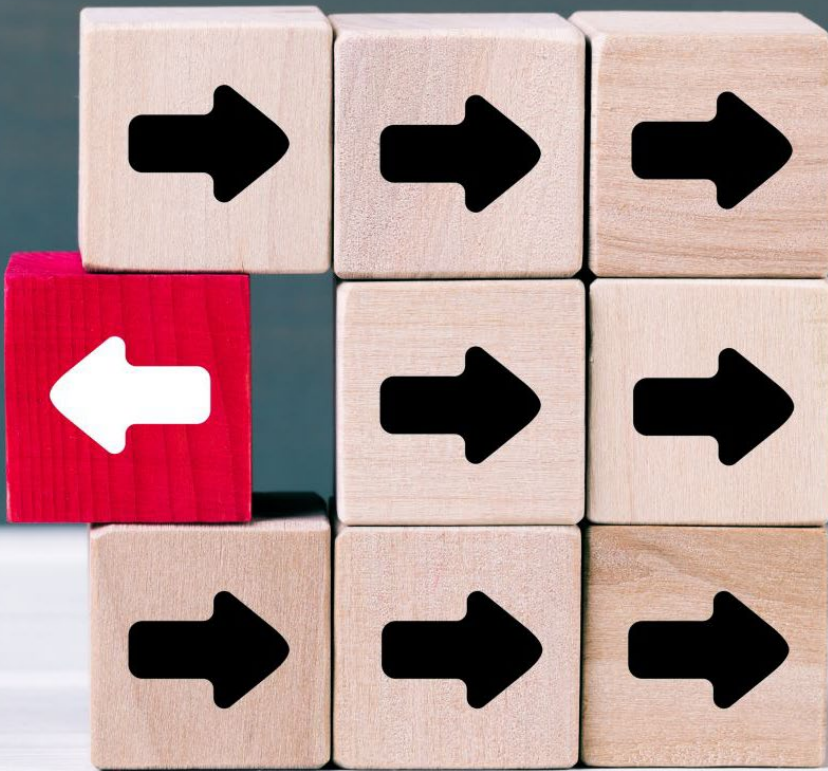
There are many ways to keep our data secure online. By taking simple steps, we can avoid the risks associated with the leaking or theft of our private data.



Do not share too much on social media

Social networking has become a way of life for many individuals, but sharing too much personal information on your social media profiles can be dangerous.

For instance, many hackers have successfully guessed passwords through trial-and-error methods, using combinations of common information (such as children's names, addresses, and other details) easily found on users' social media profiles.



Block suspicious users on social media

How many people on your social media pages do you know in person?

How do you know they are who they say they are, and how do you know their intentions?

Be familiar with the block features on social media.

Block suspicious users and know your friends!

Avoid public Wi-Fi for sensitive activity

Relying on a public Wi-Fi connection means your data can be intercepted, and any passwords or sensitive data that you send over that connection can be vulnerable to a 'man-in-the-middle' attack.

Avoid using public or open Wi-Fi for sensitive transactions, and use secure websites!

More can be [found here](https://uk.norton.com/norton-blog/2017/05/is-free-public-wi-fi.html) from the security company Norton

Web address:
<https://uk.norton.com/norton-blog/2017/05/is-free-public-wi-fi.html>



Use website privacy settings

Websites, other than social networking platforms, also offer some privacy options. YouTube, for instance, allows users to make videos private or viewable only by specified persons.

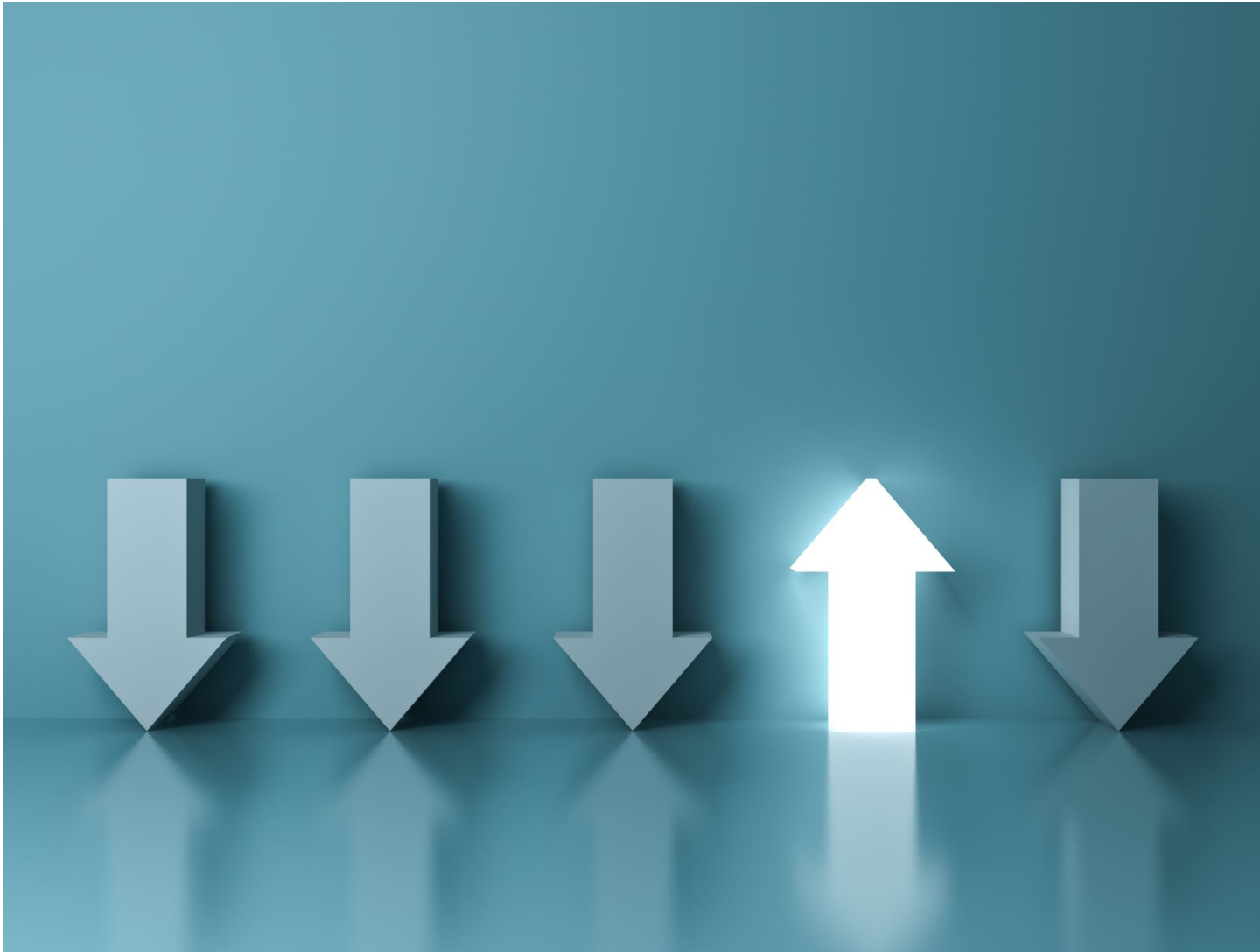


Do NOT forget to sign out

A common mistake that we have all made at one time or another.

Many websites require users to sign into access content or your account.

However, when you are using a shared or public computer, if you forget to sign out of the service you are using, the next person to that uses that computer will have full access to whatever account you were accessing.



Email security

Do not open e-mails from people you do not know or click on links in an e-mail:

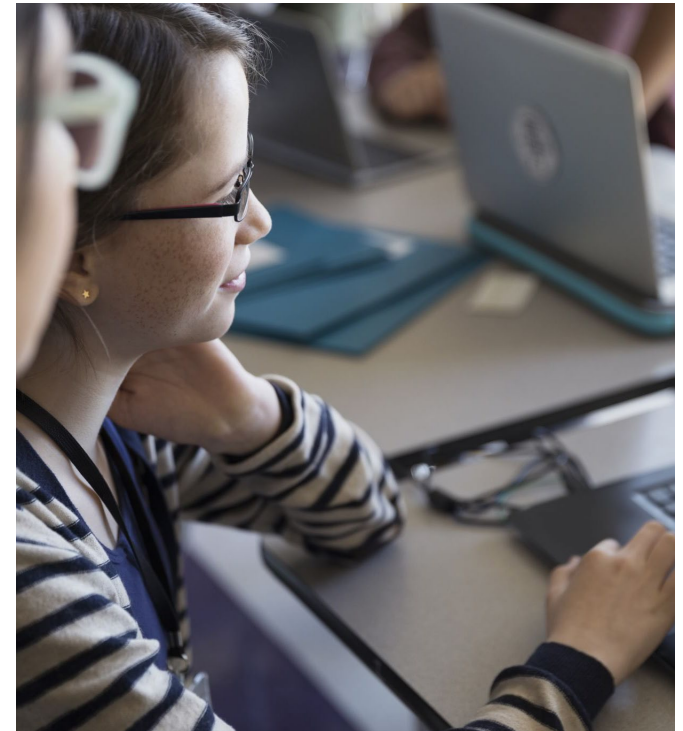
Spam e-mails and phishing scams that can lead to malware sites would come in the form of an e-mail, from someone you do not know or is not a contact.

Sometimes, though, an e-mail may look like it comes from your bank, Amazon, or eBay. It may contain a link asking you to reset your password as your account may have been hacked.

Never click on the link as it will lead to a fake site that looks identical to the real one.

You would then be asked to enter your username and password to this fake site, and before you know it, a hacker has access to your accounts.

If the e-mail looks suspicious, just delete it.



Be Mindful of Online Reputation

Any information you enter on social networking websites, accounts, or any other website could potentially be up for grabs in the event of a data breach.

In general, the information you put online contributes to your online reputation, which can affect your chances of securing employment, getting into the college or University of your choice, and create many problems if the information is unfavourable.

People will read what you post online and make assumptions about you, whether you think it is fair or not.

It is the judgemental world we live in today.

A close-up photograph of a document. At the top, there is a barcode consisting of several vertical black bars of varying widths. Below the barcode, the word 'download' is printed in a large, bold, sans-serif font. The document is slightly tilted, and the lighting is soft, creating a professional and clean look.

Careful with downloading

Do not download files from untrustworthy sites:

Many websites that offer the latest movie or game free often contain malware and viruses.

While many peer-to-peer sites are not illegal, they are a breeding ground for hackers to try to infect your computer.

A study showed that 90% of the top 30 file-sharing sites contained malware or other unwanted programs designed to harm a user's computer if downloaded.

Do not save passwords to browser

It is very easy for us to have all the passwords we use stored to a browser.

It saves having to remember them all, and type them in.

However, should someone gain access to your computer or mobile device, they would be able to easily access any accounts for which you have stored login credentials in your browser.

An illustration on the left side of the slide shows a hand with a light skin tone entering a PIN on a dark grey device screen. The screen has a white rectangular display area at the top and a 3x3 grid of black squares below it. The hand is positioned on the right side of the screen, with the index finger pointing at the center square of the grid. The background of the illustration consists of teal and brown geometric shapes.

Two-step authentication

Two-factor authentication is an additional layer of security that provides protection in the event that a hacker guesses or cracks your password.

Two-factor authentication requires a second verification step, such as the answer to a secret question or a personal identification number (PIN).

Sometimes a code will be sent to a user's mobile device, and then it has to be entered into the website.

That way if a hacker did have your password, it is unlikely they also have access to your mobile device to get the extra code needed to log in.

Don't believe everything you read



Fake news!

The internet is full of it.

Social media is guilty of allowing users to post whatever they want as a fact.

Many people have fallen victim to online scams because they believe the promises of wealth or promises of free goods that are offered.

News flash! That Nigerian Prince does not exist!

Read - link: [Nigerian Prince is not Nigerian or a Prince](#)



Task

NOW DO TASK 11