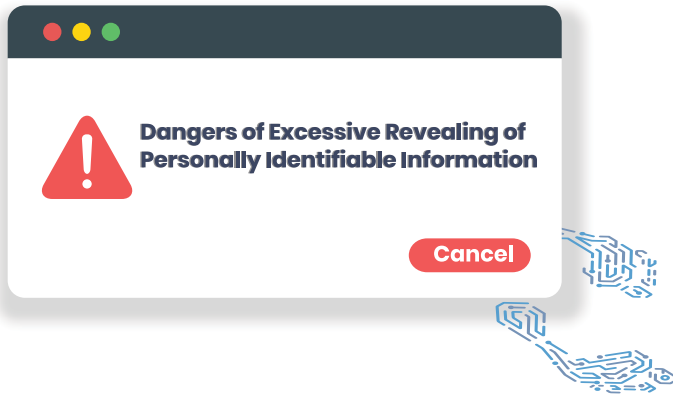




What is the difference between personal and private information?

Personal information is information that cannot be used to identify you, such as year of birth only or age, favourite food and first name only.

Private information is information that can be used to identify you and should be kept confidential. This information can be used for identity theft, phishing, and electronic fraud.

Here are some examples of private information:

- Full name
- Address
- Private phone number
- Location
- Full date of birth
- Passwords or verification codes

The questions below will help you think twice about what content you can post and share with others when posting on social media, online games or forums:

- Are you sharing something that might allow someone you don't know to identify you and get your personal information?
- Do you check privacy settings in apps to see what you allow to share with people and what is automatically shared with the app?

Consider leaving a positive digital footprint and remember, the things you share online can be there forever.

So think carefully before hitting the 'post' or 'share' button.



What is Cyber Security?

Cybersecurity is the process of protecting systems, communications, networks, and data on the Internet against cyber threats and risks resulting from cyber-attacks and acts of cybercrime that harm critical structures, infrastructures, organizations, and individuals.

What is Cyber or the Cyberspace?

Cyber is a term relating to computers or computer networks such as the internet. Cyberspace is a term that refers to the virtual computer world, in which all computer networks, digital communications, and the data generated from those communications converge over the World Wide Web "Internet".

Check and Shop!



It is considered a best practice to allocate one card for online shopping or to use a prepaid card.



Do not share your credit card information through unsecured channels or social media.



Review your account statements periodically and file a complaint with your financial institution immediately if you are suspicious of any purchase.



Be careful when sharing your banking information when shopping online and make sure that two-factor authentication is enabled.



Make sure that the website you are visiting is reliable. Cyber Criminals need to change one character to get a different URL even though it may be the same as the original one, this is called phishing.



Cyber Safety Tips for Travelers!



Ensure that the automatic connection to Wi-Fi networks feature is disabled on your devices.



Practice caution when connecting to public Wi-Fi in hotels, airports, or public cafes, and acknowledge that the use of free Wi-Fi is limited to checking flight information or finding directions to your destination. Avoid making any banking transactions or send or receive sensitive data in order to protect your privacy.



If you are connected to a public network, make sure to use only "https" sites and avoid online shopping or accessing any sensitive data to avoid any security breach.



Make sure to back up your devices before using them on your trips and update your devices periodically or activate the automatic update feature.