

PERSONAL INFORMATION

Whether we realize it or not, living in today's modern and connected world requires us to constantly share our personal information with people we trust and those whom we don't know so well. For example, the Lembaga Hasil Dalam Negeri (Inland Revenue Board) requires its eligible Malaysians to update their personal information through its portal to keep their information current for tax and rebate purposes. Another example is online shopping sites such as Lazada, Amazon.com, Lelong.com, etc. where buyers are required to share their accurate personal information to ensure the safe delivery of the goods. Users are required to share our information when signing up for email and social media accounts.

Unfortunately, our personal information that we share online is potentially open to abuse by people with bad intentions. Cyber criminals can steal your information and.

- Pretend to be yourself online;
- Make unauthorized bank or credit cards transactions;
- Use your medical insurance to pay for their own treatments;
- Make profit by selling your information to other people; or worse,
- Pose physical harm to you or your loved ones.

There are many ways Internet users can practice privacy control. Here are some:

Protect Your Personal Information

Unless you receive an official request from the authorities, do not give away your personal information such as your full name, identity card number, phone number, address, or bank account number. It may bring unwanted attention to yourself and threaten your safety.

Verify The Request

Know who you are giving your personal or financial information to and what would they do with it. If you received an urgent request (through email, phone or Internet) for your information from a company that claims to have your subscription, do not comply immediately or click any links in the email. Call the company's customer service number that you can get from its official website or your account statement and ask them about the matter.

- **It's Not What It Seems**

Beware of those psychological tests or juicy gossips sites that always require you to fill up their form with personal information before you get to the page that you desire. The sites might be run by cybercriminals who uses these avenues to steal victims' information and commit Internet related crimes, including hacking into your online accounts or devices.

- **Must I Share Everything?**

Refrain from posting too many photographs of yourself or your family members, especially inappropriate photos. Switch off webcams after use.

- **Location Sharing**

It is a feature that is available on most social media sites for users to 'check-in' to a particular location. It might be called differently on different platforms (for example, WhatsApp Live or Facebook check in) but it functions similarly. While it is a great feature to record where you were, unsafe usage of this feature might allow stalker to track your whereabouts. Photos with you in it that are tagged by your friend is another way a stalker can keep track of you.

- **Managing Privacy Setting**

You can manage your privacy settings so that only people whom you trust, like family and friends, can see what you post and share online.

- **Disposing Personal Information Safely**

Once your devices have outlived their usefulness, they are usually discarded without any safety precaution. Users often forget to delete their files and personal information, in turn putting their financial and private lives at risk. You should wipe all personal data from games consoles, tablets and smartphones and then perform a factory reset.

The specific tools or procedures needed might vary depending on the type of device, so it is important to research this for each device. Also, remember that some devices might include storage areas that aren't affected by the device's erase functions. If the device includes PC-compatible storage drives (e.g., SD cards), connect them to your PC and securely erase the data. For PCs, don't just rely on the "Delete" function or even formatting, since these will not actually remove data from the drive. Instead, you should use a program that removes data by overwriting the data multiple times.