H1: The Danger of Dark Web: Have You Been Pwned?

The dark web is an underground network of websites and services that exist beyond the reach of traditional search engines. It is a part of the deep web, which also includes sites and services not indexed by search engines.

Visual:

Surface/Open Web
Part of the internet that can be accessed by anyone using a web browser. It includes websites that are indexed by search engines, as well as password-protected websites.

Deep Web
Part of the internet that is not indexed by search engines. It includes websites that require a login, as well as databases and other information that is not publicly available.

Dark Web
Part of the internet that is intentionally hidden and is only accessible using special software. It includes illegal websites, such as those that sell drugs or weapons, as well as websites that host child pornography.

Why You Should Protect Your Personal Information Online

The dark web operates on the principle of anonymity and privacy. It uses encryption technology to make sure that users' identities remain anonymous while they navigate the darknet. This makes it difficult for law enforcement agencies to trace activities happening on the dark web.

Being a hidden network of websites and services, the dark web is often used for illegal activities such as drug trafficking, money laundering, and cybercrime. It has become increasingly popular in recent years due to its anonymity and the ability to access content that would otherwise be inaccessible. Criminals use it to carry out their activities without being detected by law enforcement agencies.

What Personal Data Can Be Found on the Dark Web?

- Passports
- Personal IDs
- Driving licences
- Email

- Payment card data
- Mobile phone numbers
- Online accounts
- Bank account logins
- Crypto accounts
- Other personal data

According to data analysed by NordVPN, personal email data from Malaysia is among the most affordable worldwide, costing RM43.89 per lot on average. Malaysian ID data costs RM43.89, and passports are the cheapest at only RM40.86. Note that even hacked accounts such as Facebook, Gmail and even Netflix accounts are being sold on the dark web.

What Happens if Your Personal Data is Available On the Dark Web

Risk of Identity Theft

Identity theft occurs when someone uses your personal information without your permission in order to commit fraud or other crimes. This can include opening new credit accounts in your name, making unauthorised charges on your existing accounts, or even taking out loans in your name.

Targeted by Scammers

Scammers may contact you via phone or email and pretend to be from a legitimate company in order to obtain additional personal information from you. They may also try to sell you products or services that you do not need.

Email Account May Be Hacked

If your email account is found on the dark web, it may be hacked by someone who wants to gain access to your personal information. Once they have access to your email account, they can read your emails, change your password, and even send emails in your name. This can lead to a loss of privacy and even identity theft.

Credit Score Affected

Your credit score could be seriously harmed and your prospects of being approved for credit are at risk if these fraudsters take out credit in your name. In the future, you might have trouble having your applications for credit cards, personal loans, or mortgages approved.

Tips to Protect Your Personal Information Online

1. Keep Your Software Up to Date

Software updates often include security patches that can help to protect your computer from new threats. Out-of-date software can be a security risk as it may contain vulnerabilities that have been patched in newer versions.

2. Use a Secure Password Manager

A password manager is a program that helps you to create and store strong passwords for all of your online accounts. This way, you only need to remember one master password, and the password manager will fill in the rest.

3. Use Two-Factor Authentication

With 2FA enabled, you will need to provide not only your username and password, but also a second piece of information, such as a code from a mobile app or an email address. This makes it much harder for someone to hack into your account, even if they have your password.

4. Be Careful What You Click

Be very careful about what emails you open and what links you click, even if they appear to come from a trusted source. If you're unsure about a link or attachment, you can hover over it with your mouse to see where it would really take you before clicking.

5. Use a VPN

A VPN (virtual private network) is a tool that can help to improve your digital security by encrypting your internet traffic and hiding your IP address. When you use a VPN, all of the data that is sent between your computer and the VPN server is encrypted, making it much more difficult for anyone to intercept or read it.

How Do We Know If Our Information is Already on the Dark Web

You can use a variety of apps to check whether your information is on the surface web, on the dark web, or has been exposed in a data breach. Experian's free dark web scan can find your

email address and phone number, and its personal privacy check can search individuals search websites for your information.

> Need link and CTA

PSA: How to Report Phone Scammers In Malaysia

You can call the National Scam Response Centre (NSRC) at 997 to report online financial scams.

Remember that NSRC, or agencies under NSRC or banks will not call you to ask for private banking details such as PIN, TAC and OTP. Always make necessary checks to verify the facts when contacted by such parties. Call NFCC at 03-88613830, police at 03-26101222 and BNM at 1-300-88-5465 for further details on NSRC.