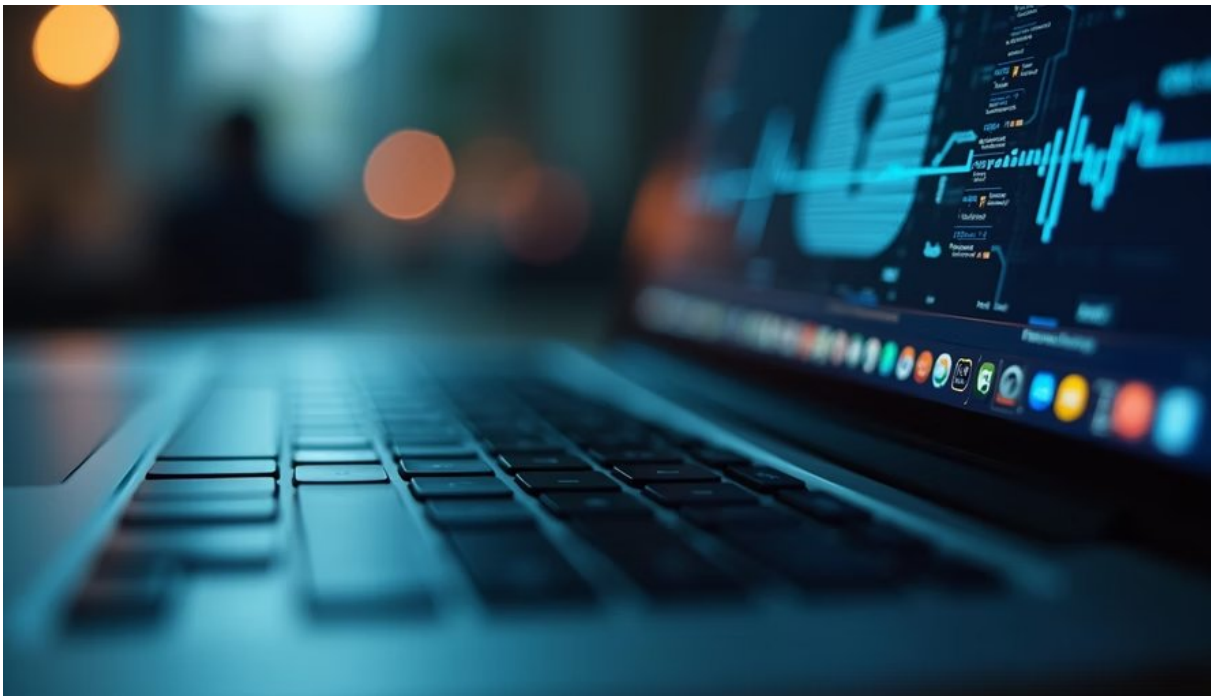


Essential Tips for Safeguarding Your Personal Information Online

Programs @ The Blue Marble · 3 min read

In today's connected world, protecting your personal information online is more critical than ever. Cybercriminals constantly seek ways to steal sensitive data, which can lead to identity theft, financial loss, and long-term damage to your reputation. Knowing what information to keep private and how to shield it effectively can save you from serious trouble. This post highlights key areas where you should exercise caution and offers practical advice to keep your personal details safe.



Keeping personal information secure on a laptop

Keep Your Social Insurance Number Safe

Your Social Insurance Number (SIN) is one of the most sensitive pieces of personal information you have. It is used by government agencies, financial institutions, and employers to identify you. Sharing your SIN unnecessarily can expose you to identity theft or fraud.

- **Never share your SIN on social media or public forums.** Even partial exposure can be risky.
- **Only provide your SIN when absolutely required.** For example, when applying for government benefits, tax purposes, or employment.
- **Verify the legitimacy of requests for your SIN.** If you receive an unexpected call or email asking for your SIN, confirm the source before sharing.
- **Store physical documents containing your SIN securely.** Avoid carrying your SIN card or documents with you unless necessary.

By treating your SIN like a password, you reduce the chances of it falling into the wrong hands.

Avoid Oversharing on Social Media

Social media platforms encourage sharing personal moments, but oversharing can reveal more than you intend. Details like your birthdate, address, or daily routines can be used by criminals to guess passwords or answer security questions.

- **Limit the personal information you post.** Avoid sharing your full birthdate, home address, phone number, or vacation plans.
- **Adjust privacy settings.** Restrict who can see your posts and personal details to trusted friends and family only.
- **Be cautious about "check-ins" or location tags.** Publicly announcing your location can alert criminals that your home is empty.
- **Think before posting photos.** Images can reveal details like your car's license plate, street signs, or valuable possessions.

Remember, once information is online, it can be difficult to remove completely. Keeping your social media presence minimal and private helps protect your identity.

Protect Your Banking Details

Banking information is a prime target for fraudsters. Losing control of your bank account details can lead to unauthorized transactions and financial loss.

- **Never share your bank account number, PIN, or passwords** online or over the phone unless you initiated the contact.

- **Use strong, unique passwords for online banking** and change them regularly.
- **Enable two-factor authentication (2FA) whenever possible.** This adds an extra layer of security by requiring a second form of verification.
- **Monitor your bank statements frequently.** Look for any suspicious or unfamiliar transactions and report them immediately.
- **Avoid using public Wi-Fi for banking transactions.** Public networks are often unsecured and vulnerable to hackers.

Taking these steps helps keep your financial information out of reach from cybercriminals.



Smartphone showing secure banking app interface

Recognize Identity Theft Warning Signs

Identity theft can happen without your immediate knowledge. Recognizing early signs can help you act quickly to minimize damage.

- **Unexpected bills or charges.** Receiving bills for accounts or services you did not open.
- **Denied credit or loans.** Being turned down for credit despite a good history.
- **Unfamiliar accounts on your credit report.** Regularly check your credit report for accounts you don't recognize.

- **Receiving calls or letters about debts you don't owe.**
- **Missing mail or important documents.** This could indicate someone is intercepting your mail to steal information.

If you notice any of these signs, contact your financial institutions and credit bureaus immediately. Consider placing a fraud alert or credit freeze to protect your credit profile.

Programs @ The Blue Marble