Microsoft

The Netizens' guide to a Cyber-Secure India

Issued in public interest by Microsoft India

The Indian Netizens' Pledge

WE, THE NETIZENS OF DIGITAL INDIA,
solemnly resolve to play our part in securing her virtual borders.

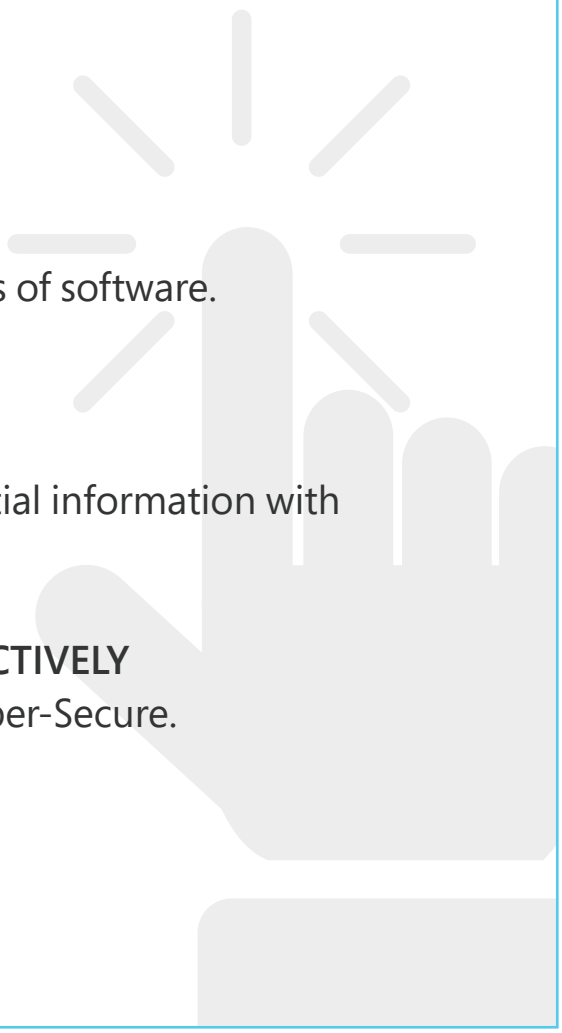
WE PLEDGE TO ACT
responsibly when navigating the online space.

WE PLEDGE TO BE WARY
of suspicious-looking emails.

WE PLEDGE TO TAKE
full control of our devices
by updating to the latest versions of software.

WE PLEDGE TO USE
strong passwords everywhere.
And to never share our confidential information with anyone.

LET'S PLEDGE TO WORK COLLECTIVELY
towards making Digital India Cyber-Secure.



Index

Chapter 1:
Towards Stronger Passwords

Often, the one thing standing between you and cyber criminals is your **Password**.

Maximum data breaches continue to take place as a result of weak, default or stolen passwords. Create strong passwords – for all your online avatars across all your devices.

Here are some best practices to keep in mind:

- Always go for unique and hard-to-guess passwords.
- Always create passwords that are a mix of uppercase and lowercase letters, numbers and even special characters.
- Use different passwords for different accounts.
- Never share your passwords with anyone.
- Never save your passwords in text or in writing, and keep it in a place that's accessible to everyone.
- If you lead an organization or look after the IT function in a large enterprise, you need to enable multi-factor authentication for your teams.

Chapter 2:
Securing your PCs and Mobiles

Every aspect of our lives has gone digital, spread across platforms and devices.

Use your PCs, mobiles and other personal devices with utmost caution. Here are some ways to keep your devices protected and your data secure:

- Always invest in devices with genuine software applications.
- Subscribe and download the latest updates and patches to keep your operating system secure.
- Backup your data on the cloud and password-protect your critical files across your devices.
- If you lead the IT function in your organization, enable highest levels of permissions and security across all users and devices connected to the organization's infrastructure.

Chapter 3:
Being Safer Online

All of us enjoy the benefits that come with having an online presence. And yet, we must be wary of the dangers that lurk at the turn of every web page, on the unseen side of every hyperlink.

Here are some basic points to keep in mind while navigating the online space:

- Be alert when browsing the Internet. Even opening or viewing suspicious links can compromise your PCs and mobiles.
- If you are undertaking an online financial transaction, always look for 'https' in the URL of the checkout page.
- Always use privacy settings to restrict access to your personal information on social media sites.
- Delete old accounts that you don't use anymore.
- Access your bank's website by manually typing its URL in the address bar and never directly from an email or a text message.
- Never respond to pop-up ads that may come up on your screen. To close such pop-ups from the task manager, press Alt+Ctrl+Delete.

A Final Word

Stay alert and stay vigilant.

Empower your family and friends with the know-how with which they can secure their digital interactions.

Visit www.microsoft.com/security to learn more about security features in-built across Microsoft's products and solutions.

Follow the conversation on Twitter with **#MSFTSecure**