



Defend our Digital workspace

Protect your Password

- Use Strong Passwords :Blend upper and lower case letters,numbers and symbols.
- Switch Regularly : Update all Passwords every 3-6 months.
- Avoid Recycle : Do not use Identical passwords across multiple websites.



Be Vigilant with Emails

- Beware of Phishing : Do not click on links or attachments if you do not know the original source
- Verify Sender : Always Check Email addresses for Authenticity
- Report Suspicious Activity : Notify your IT department if you suspect Phishing.

Always Update Software

- Update Regularly : Ensure all software, and antivirus programs are all upto date.
- Automate Update : Make sure automatic updates are enabled to stay protected against the latest threats.

Use Secure Networks

- Avoid Public Wi-Fi : Use a vpn if you must connect to a public Network.
- Secure Connections : Ensure all websites you visit use HTTPS for secure communication.



Safeguard Devices

- Lock Screens : Always lock your Devices when not in use.
- Use Authentication : enable two-factor authentication for added security.
- Monitor Devices : Keep track of all your devices and report any lost or stolen items Immediately.

Clear Your Cache

Dont misjude your browser's cache and how much information it has about you. Saved cookies, searches, and Web history could have your home address, personal information, and other personal data.(Rubenking,2024)