Cybersecurity Tips & Tricks: Security Guidelines for Using Public Wi-Fi

This awareness campaign emphasizes the importance of secure Wi-Fi usage in public spaces. While public Wi-Fi networks offer convenience, they can expose users to significant security risks, including data theft and unauthorized access. By adhering to the best practices outlined in the infographic below, you can safeguard your personal information and ensure your privacy. Remember, staying vigilant and implementing simple security measures can dramatically reduce your risks when using public Wi-Fi.

IMPORTANT!

BEST PRACTICES FOR PASSWORD SECURITY

CREATE STRONG PASSWORDS

- Use at least 12 characters.
- Include uppercase and lowercase letters, numbers, and special characters.
- Avoid easily guessable information like names or common words

USE UNIQUE PASSWORDS

- Ensure each account has a different password.
- Do not reuse passwords across platforms.

CHANGE PASSWORDS REGULARLY

- Change passwords periodically.
- Change your passwords right away if you suspect a breach.

ENABLE MULTI-FACTOR AUTHENTICATION (MFA)

Revision #2

Created Thu, Aug 29, 2024 12:48 PM by FAZILAH BT. BASARUDDIN

Updated Fri, Sep 11, 2026 10:05 AM by FAZILAH BT. BASARUDDIN