SAFE FROM TWO-FACTOR AUTHENTICATION FRAUD

- Cybercriminals often merge malware with on extension or plugin.
- Avoid installing any extension or plugin from external sources.
- Always validate them by reading reviews and through an extensive online search.
- Never save any sensitive information like login credentials or financial details in the browser.

USE STRONG PASSWORD

- Make them LONG and STRONG!
- Never share your passwords
- Different service=Different password.
- Use 2-step authentication where available.

RECOGNIZE AND REPORT PHISHING/ VISHING/ SMISHING

VISHING-

- This term comes from the combination of two words: voice and phishing. It refers to the type of threat that involves a fraudulent phone call using information previously obtained online.

- A customer should never reveal this kind of information to anyone because they are the key to authorizing transactions.

- The bank will never contact customers to request sensitive and confidential information on passwords and pins.

SMISHING-

- This threat takes place when the customer receives a text message supposedly from their bank saying that a suspicious purchase was made with his or her credit card.

- To avoid smishing is to never pay attention to messages requesting data, a phone call or an operation**.**

PHISHING-

- It involves sending fraudulent emails sending customers to a fake website that looks like their banks.

- Defence against phishing is using common sense to not provide confidential information.

- Banks never send emails like "you won a prize" or "unblock your account.

HOW TO PREVENT ONLINE FINANCIAL FRAUDS

- Do not contribute to crowd funding without verifying and check if you know other Backers.
- Do not reveal personal financial details s on social media sites.
- Do not befriend anyone you don't know on social media.
- Shop through established e-retailers with transparent exchange and return policies.

UPDATE YOUR SOFTWARE

- Software and application updates contain important security fixes that can help keep your devices safe from cyber criminals.
- If your software and apps are not up to date, you run the risk of allowing cyber criminals to find and use these vulnerabilities for their malicious intents.
- Updates can also deliver bug fixes and improvements, as well as add new features to your software and apps.

BE CYBER-SMART! HABITS TO STAY CYBER-SAFE

- Think twice before clicking on links or opening attachments.
- Verify requests for private information.
- Protect your passwords.
- Protect your stuff!
- Keep your devices, browsers, and apps up to date.
- Back up critical files.
- Delete sensitive information when it's no longer needed.
- If it's suspicious, report it!

****