10 tips to

# Secure Your Devices

VISRAM SECURITY
your privacy is our concern

## Strong Passwords & Biometrics

A strong password protects you from unauthorized access when your devices are lost or stolen. In addition, Biometrics allows you to unlock your device quickly and conveniently.

Action

Use at least 10 characters that are memorable to you and difficult for others to guess.

AVOID using the numerical PIN or pattern swipe password options, as they can be easily seen by someone looking over your shoulder.

## Activate Auto Lock

Auto-lock feature ensures your device automatically locks after a specified period of inactivity.

Action

Set the lockout time between 2 to 5 minutes

## Auto Erase After Failed Login Attempts

Protect your DATA from password-guessing attacks by enabling the auto-erase security feature.

Action

Enable “Erase Data” on Apple and “Auto factory reset” on Android devices (only available on select Android devices).

## Auto update operating system (OS) and Applications (APP)

Auto updates ensure your devices automatically receive the critical OS and APP security patches that keep your devices secure and up-to-date.

Action

Enable auto-update for BOTH OS and APP (settings found in separate locations).

## Install APPs from Official Apple or Google Marketplaces

Use ONLY used trusted sources to avoid the millions of malicious applications built to monitor your actions, steal your information and send harmful text messages, etc.

Action

Ensure that you ONLY download apps from trusted marketplaces like Apple’s “App Store” and Google’s “Play Store.”

Read APP reviews and details around privacy + security BEFORE you download them.

If you are still uncertain, ask for help OR don’t install the app.

Due to Android’s open architecture, it is <u>HIGHLY recommended</u> you perform additional internet searches about that app to be sure it is safe to install.

## Enable “Find My Device”

If your device is lost or stolen, your data can be used maliciously to target you, your family, your friends and your business. “Find My Device” allows you to locate and retrieve or erase your device.

Action

Enable the remote find feature on your device to allow you to use Apple’s “Find My” and Google’s “Find My Device.”

## Install Security Software

Security software provides an essential layer of protection. Some features include
- scanning for malicious APPs
- protection against phishing attempts
- blocking malicious websites
- remotely find and erase your device

Action

Install reputable security software that is highly reviewed, receives regular updates and has a long history.
Security software is HIGHLY recommended for Android devices due to its open architecture and ability to install software from a more extensive array of sources beyond the official Google Play Store.

## Configure Privacy and Security Settings

Default factory settings are NOT secure or private as they expose your location, network, contact, calendar, camera microphone, and other info to <u>ALL</u> APPs that request it.

Action

<u>iOS</u>: Review the options under “Apple ID,” “Content & Privacy Restrictions,” “Face ID & Passcode,” “AirDrop,” “AirPlay & Handoff,” AND “Privacy & Security,” then disable (or limit) access to APPs and services that request access to your location, camera, microphone, contacts, etc.

<u>Android</u>: Review the options under “Privacy,” “Location”, “Find My Device,” and “Permissions Manager,” then disable (or limit) access to APPs and services that request access to your location, camera, microphone, contacts, call logs, etc.

Both iOS and Android:

- Bluetooth – turn off when not being used
- Camera – turn off “location services” (iOS) or “location tagging” (Android)

## Password Manager

Password managers assist in creating secure passwords, support 2FA, provide some protection against phishing attacks, proactively alert you to change your password after a data breach, provide backup features and allow for synchronization across multiple devices/computers.

Action

Install and use a reputable password manager to create, store, backup and synchronize your passwords across your computers and devices.

## Think Before You Click, Open, Download or Install

Many unexpected messages that direct you to perform these actions may be attempting to steal your personal information and infect your devices.

Action

STOP and THINK BEFORE clicking on a link, opening an attachment, downloading a file, or installing an APP.

Contact the business via their official website, phone number or email address, if you are suspicious about the message you received from them.

Copying and pasting the message, website or APP name into a search engine (e.g. Google) may reveal if it is malicious.

If in doubt, get help and training from knowledgeable sources.

Our Core Values…

## IT’S THE EXPERIENCE

The most important part of the Visram Security experience is that we focus on building a relationship with you, your family and your team.

We learn about what is important to you then together, we build and implement a customized protective strategy.

## WE PROTECT FAMILIES

While others focus on companies, we protect families.

Each family and their businesses are unique and require a bespoke solution.

We bring ten years of experience protecting multi-generational HNW families and their operating businesses.

## OUR MISSION

Our goal is to transform families worldwide into becoming resilient against attack.

We want our families to have the same robust protection and support currently available to businesses.

## Contact Us:

✉ Info@VisramSecurity.com

🌐 VisramSecurity.com

in /VisramSecurity

🐦 @VisramSecurity

10 tips to

# Secure Your Devices

Device security and privacy is paramount to keeping you, your family and your business safe from attackers.

Use these tips to begin protecting your privacy and increasing the security of your devices.

VISRAM SECURITY
your privacy is our concern