iCreative

tel: 877-392-8200
www.theicreative.com

DIGITAL SECURITY ESSENTIALS

OBJECTIVES:

1. *TO UNDERSTAND THE BIG PICTURE*
2. *KNOWING HOW TO TAKE ACTION*
3. *LEARNING ABOUT HELPFUL RESOURCES*

Digital Security Made Simple

Part 1 — The Big Picture

- What “digital security” actually means
- The #1 truth: Most scams target people, not computers
- Why seniors are targeted (and why it’s not your fault)

Part 2 — Locking Down Your iPhone & iPad

- Passcodes & Face ID
- Stolen Device Protection
- iCloud & backups
- Safari and privacy protections
- Location sharing & tracking risks

Part 3 — Securing Your Mac

- Login passwords & auto-login dangers
- FileVault (disk encryption)
- Safari & browser safety
- Software updates
- Fake “virus warning” popups

Part 4 — Scams You Don’t Expect

- Phone calls that look real
- Texts from “Apple,” “Amazon,” “Bank,” or “USPS”
- Email tricks that fool smart people

- QR-code scams
- Fake tech support popups
- Gift card scams

Part 5 — What To Do When Something Feels Wrong

- Stop
- Don’t click
- Don’t talk
- Who to call (and who not to)

Part 6 — Always buy iPad Pro, which features Face ID

- NEVER put your device passcode into your device in public
- The ONLY exception is when you reboot your device
- If you do not “get along with” Touch ID you will get in the habit of entering your device passcode every time (worst case scenario)
- Be mindful of your surroundings whenever you need to use your device passcode

Part 7 — Use the Passwords App and Secure Notes

- Apple’s Passwords App securely encrypts your passwords
- It synchronizes them across all of your devices
- FaceID can be used to open the Passwords App and Secure Notes in the Notes App
- Do not keep sensitive information in the Contacts App

Digital Security for Apple Devices

A Simple, Calm Guide for iPhone, iPad, and Mac

The Most Important Thing to Know

Apple, your bank, Amazon, and the government will NEVER call you asking for passwords, codes, or gift cards. Not ever. No exceptions.

It is important to establish this from the get-go. They They will not ask for these things over the phone, via a text message or via an email.

PART A: iPhone & iPad — Essential Security Settings

Turn ON Stolen Device Protection (Very Important)

Why:

If your phone is stolen, this prevents thieves from changing your Apple ID.

Steps:

1. Open Settings
2. Tap Face ID & Passcode
3. Scroll down
4. Turn ON Stolen Device Protection

Protect Your Apple ID (Your Digital Identity)

Steps:

1. Open Settings
2. Tap your name at the top
3. Tap Sign-In & Security
4. Make sure Two-Factor Authentication is ON
5. Confirm your trusted phone number is correct

📌 Apple will never ask for your 6-digit verification code.

PART B: iCloud, Safari & Privacy (iPhone/iPad)

iCloud Backups (Protection Against Loss & Ransom)

Steps:

1. Open Settings
2. Tap your name

3. Tap iCloud
4. Tap iCloud Backup
5. Turn ON

💡 Unknown fact: Many ransomware scams fail if backups exist.

Safari Security Settings

Steps:

1. Open Settings
2. Tap Safari
3. Turn ON:
    - Block Pop-ups
    - Prevent Cross-Site Tracking
    - Fraudulent Website Warning

If Safari says “This site is dangerous,” believe it.

Location Sharing — What Most People Don’t Know

Steps:

1. Open Settings
2. Tap Privacy & Security
3. Tap Location Services
4. Review apps
5. Change most to While Using App

📌 Unknown fact: Flashlight, games, and coupons do NOT need your location.

PART C: Mac Computer Security

Turn OFF Automatic Login

Steps:

1. Click Apple Menu
2. Choose System Settings
3. Click Users & Groups
4. Turn OFF Automatic Login
5. Always use Touch ID
6. Be mindful of your surroundings

Turn ON FileVault (Encrypts Your Data)

Why:

If your Mac is stolen, your files stay unreadable.

Steps:

1. Open System Settings
2. Click Privacy & Security
3. Scroll to FileVault
4. Turn ON
5. Save the recovery key safely

Fake Virus Warnings (Extremely Common)

🚫 Messages like:

- “Your Mac is infected!”
- “Call Apple Support immediately”
- “Do not shut down!”

These are always scams.

What to do:

- Close the browser
- Restart the Mac
- Do NOT call any number on screen

📌 Apple does not display phone numbers in popups.

PART D: Scams & Tricks Seniors Don't Expect

The "Helpful Stranger" Scam

- "I'm calling to help you"
- "Your account is in danger"
- "We need to act fast"

Rule: Urgency = scam

Gift Card Requests

- Apple
- Amazon
- Target
- Walgreens

Truth: No legitimate company accepts gift cards as payment.

Text Message Scams

- "Your package is delayed"
- "Unusual bank activity"
- "Confirm your account"

What to do:

- Don’t tap
- Delete
- If worried, open the official app yourself

QR Code Scams (New & Dangerous)

- Fake parking
- Fake menus
- Fake payments

Rule: Only scan QR codes you personally trust.

Phone Call Rule (Golden Rule)

If you didn’t place the call, do not trust it.

Hang up. Call back using a number you already have saved.

If Something Feels Wrong — Do This

1. Stop
2. Don’t click
3. Don’t talk
4. Don’t send money
5. Ask someone you trust

💬 Smart people get scammed. Cautious people don’t.

Consider These helpful products:

Here are five well-known, legitimate services that can help you stay safe on your Apple devices by monitoring identity threats, protecting personal information, and aiding recovery if something goes wrong:

1. **Aura** – Comprehensive identity theft protection with dark web monitoring, account alerts, and fraud resolution support. Known for strong credit monitoring and insurance coverage.
2. **Identity Guard** – Trusted identity protection service that offers monitoring of personal data, credit monitoring, and alerts for suspicious activity.
3. **LifeLock (by Norton)** – Long-established identity protection brand with credit monitoring, identity restoration support, and insurance; includes additional online security tools when bundled with Norton services.
4. **NordProtect** – A newer but highly rated option that combines identity monitoring with dark web scanning, credit monitoring, alerts, and recovery support (often with insurance).
5. **Nord VPN** –NordVPN is a virtual private network (VPN) service that protects your internet connection by encrypting your dataand hiding your IP address. It creates a secure, encrypted tunnel between your device (iPhone, iPad, Mac, etc.) and the internet.
6. **IdentityForce / IDShield** – Reputable companies offering robust identity monitoring, credit bureau alerts, and recovery services; widely recommended for comprehensive identity protection.

These services work across platforms (including iOS) and help protect personal information, alert you to suspicious activity, and assist with resolution if identity fraud occurs — especially useful for seniors who may be targeted by scams or data breaches.

OTHER HELPFUL RESOURCES:

In macOS Tahoe, the Tips App has everything you need, literally manuals for all devices, apps and software. The most incredible resource there is!

The App icon looks like this:

Don't forget that there is a website dedicated just to this class, with downloadable versions of these files. I will also post tutorial videos of the class based on your feedback!

www.theicreative.com/security