Christer Edwards

Tech Fundamentals - Week 4

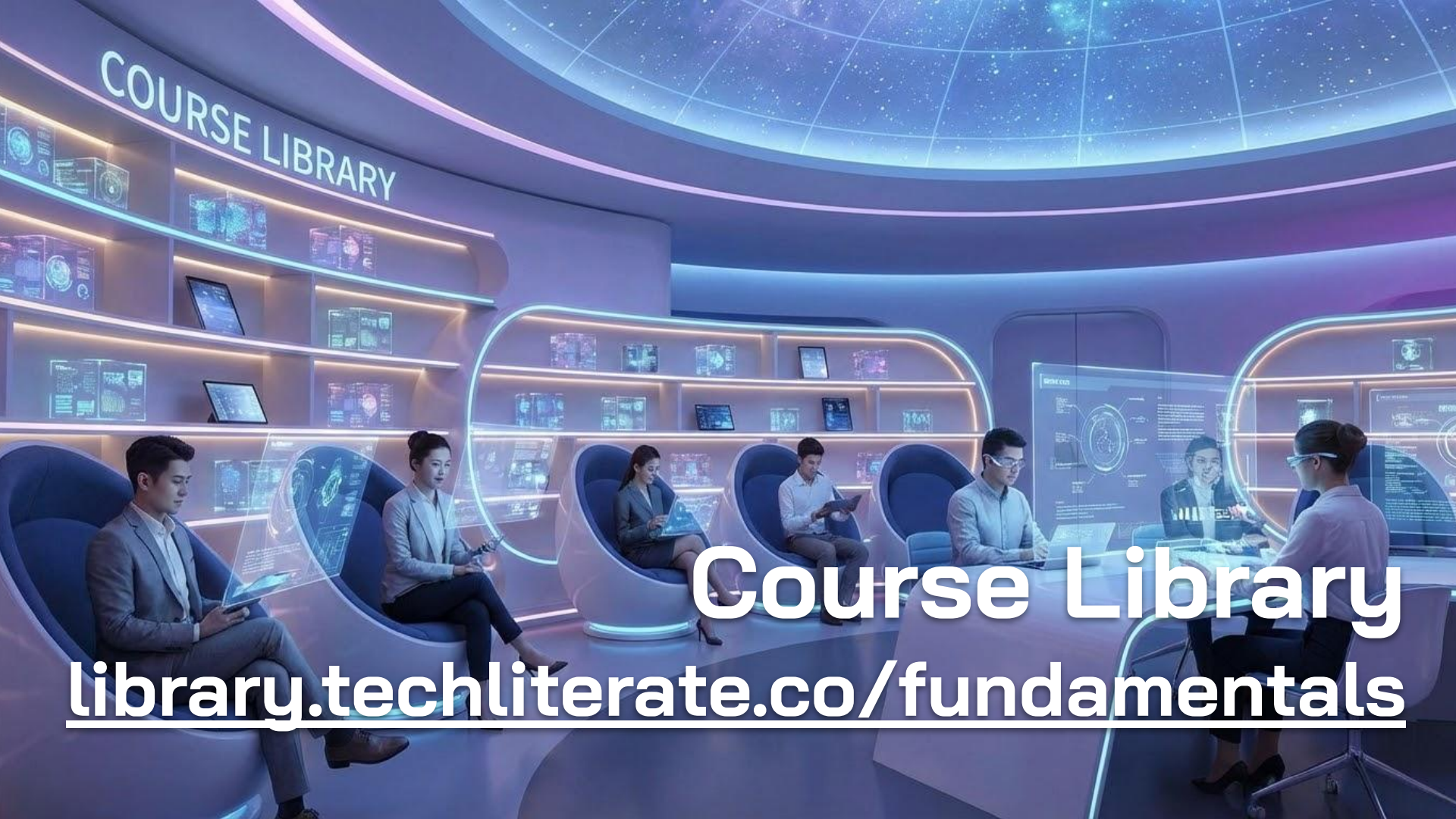
CYBERSECURITY

COURSE FUNDAMENTALS

Tech Fundamentals: Week 4

1. Understanding Data Collection
2. Password Managers / MFA
3. Software Updates
4. Phishing & Social Engineering

Week 4 Objectives



Course Library

library.techliterate.co/fundamentals


FACIAL RECOGNITION & BEHAVIORAL TRACKING
UNSECURED NETWORK & TRAFFIC MONITORING
VOICE ACTIVATION & AUDIO RECORDING
LOCATION SERVICES & APP DATA HARVESTING
Passive Data Collection
TRANSACTION DATA & PURCHASE HISTORY LOGGING
LOYALTY PROGRAM & PERSONAL DATA PROFILING

Internet cookies are small text files that websites place on your device to help the browser ”remember” your interactions between visits. Their primary purpose is to improve user experience by retaining essential data, such as keeping you logged into an account or preserving items in a shopping cart. ”first-party” cookies are helpful for functionality, but ”third-party” cookies are often used by external advertisers to follow your movements across different websites.

Cookies

Online trackers are invisible snippets of code, such as pixels or scripts, embedded within the websites you visit to monitor your activity in real-time. Unlike cookies which function like ID cards stored on your computer, trackers act like surveillance cameras that record specific behaviors, such as where you click, how long you read a page, and your mouse movements. This data is instantly transmitted to data brokers and analytics companies, who aggregate the information to build detailed profiles of your interests and habits without your explicit consent.

Trackers

https://amiunique.org/fingerprint

https://coveryourtracks.eff.org/

Device Fingerprints


Password
Management

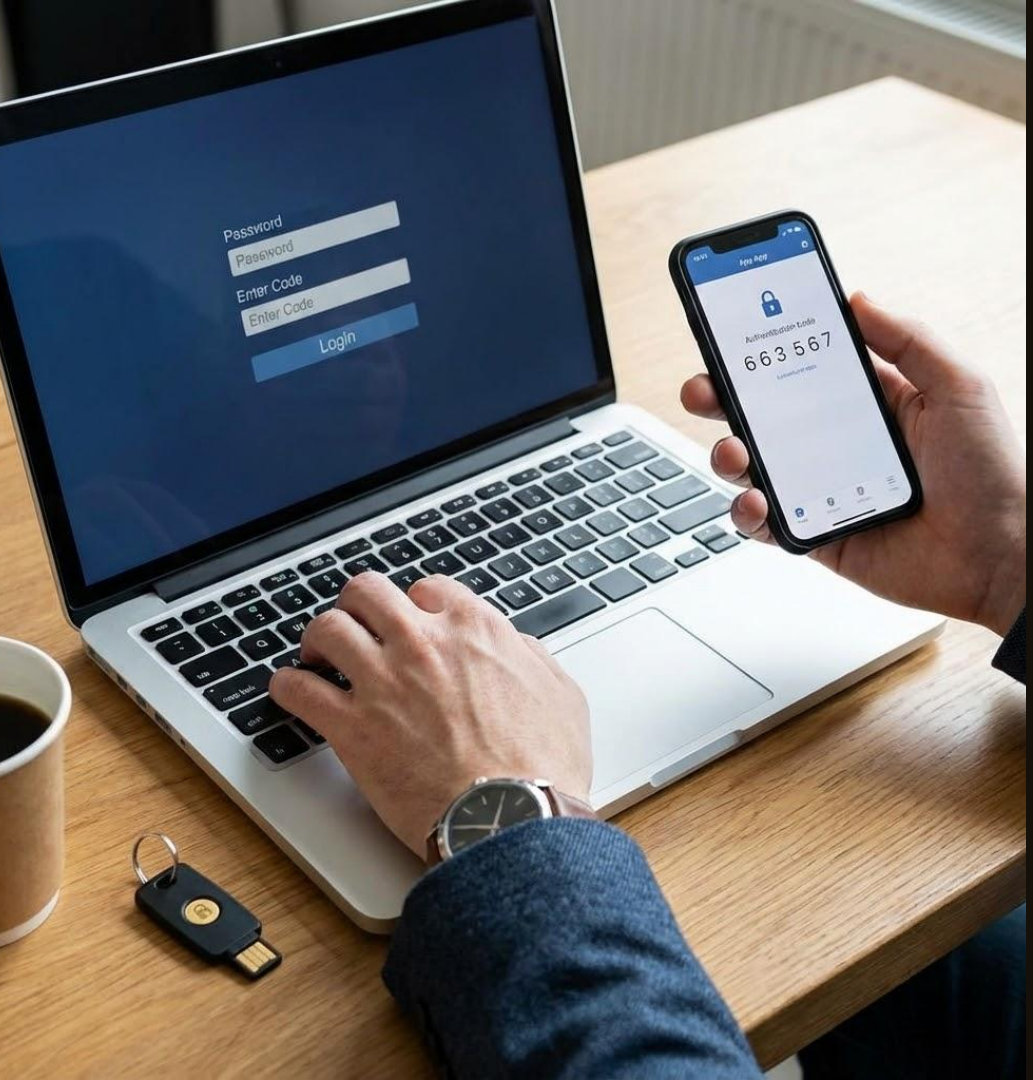
Bitwarden (recommendation)

1Password

Lastpass

Dashlane

Password Managers



Multi-factor authentication typically involves combining ”something you know” (your password) with ”something you have” (like a code sent to your phone or a hardware security key) or ”something you are” (such as a fingerprint).
MFA acts as a critical fail-safe because even if a hacker successfully steals your login credentials, they remain locked out without the second piece of evidence.

Multi-Factor Authentication

The most immediate danger is a technique called ”credential stuffing.” When a website suffers a data breach, the usernames and passwords are often dumped onto the dark web.

If you reuse your password, a breach at a minor, low-security website effectively hands hackers the keys to your most important financial and social accounts.

Avoid Reusing Passwords

Software Updates

Click the Apple icon in the top-left of the screen and select **System Settings** › **General** › **Software Update** › **Check for Updates.**

Ensure ‘Automatic Updates’ is “On”.

macOS Updates

Open the **Settings** app > **General** > **Software Update**

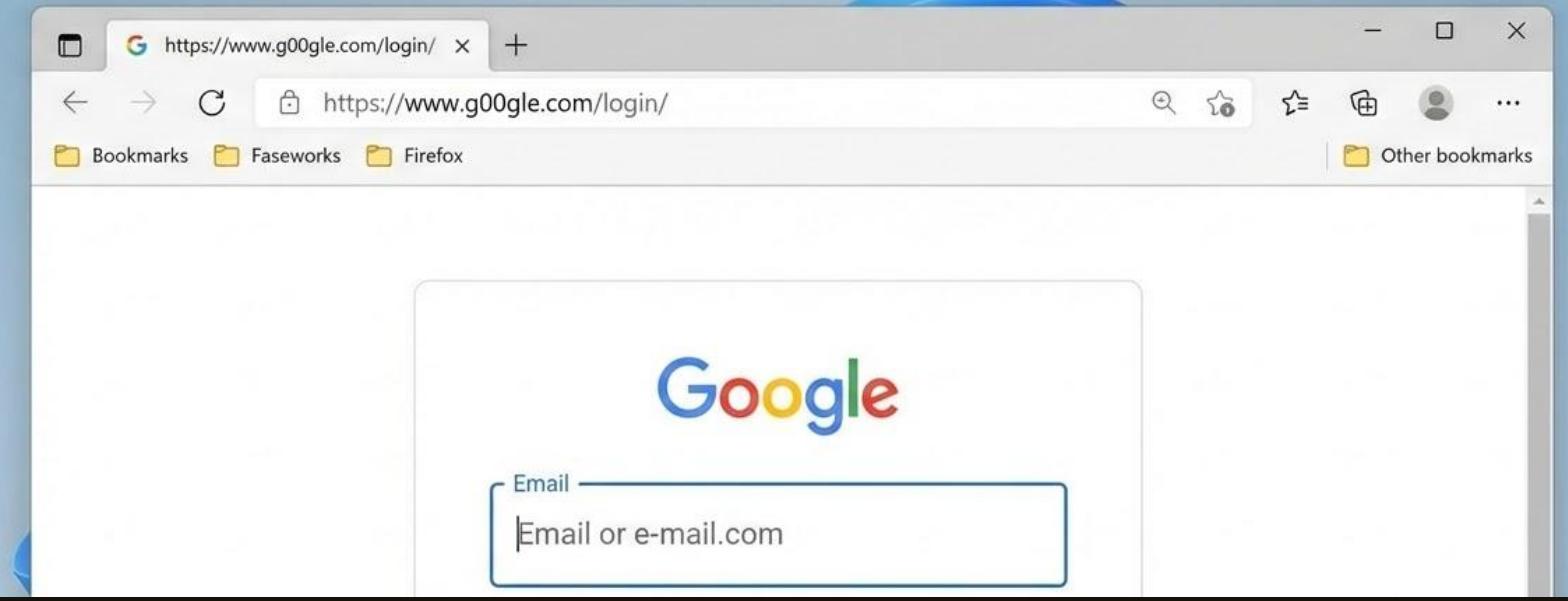
Ensure Automatic Updates is turned on

iOS

Everyone take a few minutes right now and check for available updates for laptops and mobile devices.

Remember to check for mobile app updates via **App Store** › **Account** › **Pull Down to Refresh** › **Update All.**

Check for updates



Phishing Attacks

Disguised URLs

paypall.com

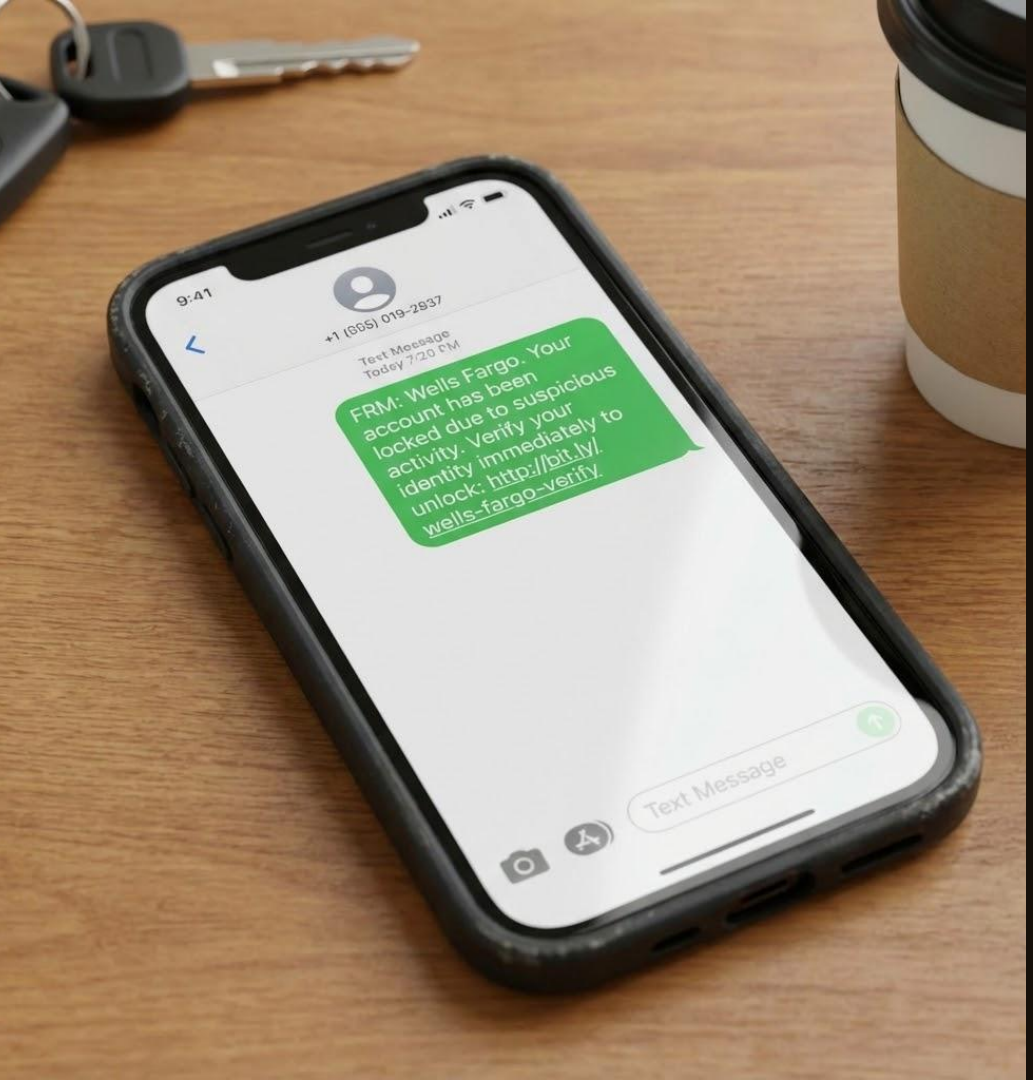
amazn.com

amazon.com.delivery-confirmation.net

paypa1.com

microsoftt.com

Examples of phishing URLs disguised as valid sites.



The number of phishing attacks against mobile devices is on the rise. These usually arrive from unknown numbers with some vague text to entice a reply.

Do not reply! This confirms that your number is valid and they'll just keep trying from different numbers after you block the first.

The best approach is Delete and Report Spam.

SMS / iMessage

What you learned this week:

1. Data collection happens anytime you use the internet.
2. Use of password managers are best practice
3. Add multi-factor authentication for sensitive accounts.
4. Phishing attacks are more common than you think.
5. Apply software & app updates when they become available.

Week 4: Recap

What you'll learn next week:

1. Cybersecurity essentials
2. Internet privacy best practices
3. Password Management
4. Two-Factor Authentication (2FA / MFA)

Week 5: Preview

If you apply the security best practices we've talked about tonight you'll be more secure than most people on the Internet.

Stay safe out there

Thanks!

If you have any questions:
christer.edwards@gmail.com
385-225-4925
https://library.techliterate.co