Willow Valley Computer Club

Member of apcug

An International Association of Technology & Computer User Groups

Project Upskill II

Protecting Data In Transit

Al Williams

March 25, 2025

Our Goal for the Project Upskill II Presentations

We’re addressing significant data security threats and offering concrete solutions. By building your awareness of potential risk, we aim to enhance your ability to protect your data.

A brief review of previous presentations

Our Goal for the First Presentation

We often focus on the visible risks to our data, like device security. However, hidden risks, such as overlooked privacy policies, can be just as damaging. Our first presentation shed light on this crucial area.

In the first presentation

We want to protect our personal information through cybersecurity but we give away our personal information by agreeing to Privacy Policies.

Review the Privacy Policies of the apps and web pages you're using to determine what personal information you're giving away.

Be aware that you're also giving away your location. You can control app access to location services, but you need an RFID device to block cell tower tracking.

Our Goals for Presentations 2, 3, and 4

To ensure the security of your personal data on your computing devices, we provided a layered security approach including cybersecurity, preventing account breaches, and ensuring the protection of your stored data.

Basic Cybersecurity Concerns – 2nd

- Vet technologies before using them
- Keep your device's operating system and apps up to date
- Ensure Antivirus and Malware Protections are active
- Avoid hardware with known vulnerabilities
- Protect the physical security of your digital devices
- Implement User Account Control to protect your computer
- Manage application permissions for privacy and security

Account Compromise Concerns – 3rd

- Formulate Strong Passwords and PIN Codes
- Cyber Smart: Use a Password Manager to Create and “Remember” Strong Passwords
- Why a Strong Password isn’t Enough: Your Guide to Multifactor Authentication
- Why Passkeys are a Good Thing
- Email Aliases are also a Good Thing
- Some Browser Extensions are a Bad Thing

Protect Data Stored on Your Devices – 4th

- Frequently back up your data to reduce the risk of permanent loss
- Encrypt the data stored on your devices
  - Encrypt the hard drive (SSD), or
  - Encrypt files
- Securely store old devices

Our Goals for the Last Four Presentations

To ensure the security of your personal data that isn’t on your computing devices, we provide ways to

protect your data in transit,
secure your home Wi-Fi,
manage your privacy and security online, and
use Virtual Private Networks (VPNs) appropriately.

Protect Your Data in Transit

- An introduction to encryption
- Communicate securely on your mobile device
- Stay safe while web surfing: Browser settings
- Stay safe while web surfing: Accessing websites securely
- Get the most out of cloud storage and services while minimizing the risk

An Introduction to Encryption

Imagine that you want to send a recipe to someone, but you want to keep the contents confidential. You decide to encrypt it.

The original recipe is in its normal, readable form.

You put the recipe into a message.

The secret code (encryption algorithm) takes your message and changes every word, ingredient, and instruction according to a complex set of rules. It turns your original recipe into a completely jumbled mess of words and symbols.

An Introduction to Encryption

The decoder ring (the encryption key) is the crucial piece of information that tells the recipient exactly how the message (recipe) was scrambled. Only someone with the correct decoder ring (correct encryption key) can reverse the process and turn the scrambled message back into the original, readable recipe.

The security of your recipe depends on you and the recipient keeping that decoder ring (the encryption key) safe and private.

The app that is involved, your browser, email, or messaging app, handles all the details of encrypting and decrypting messages.

Securing Your Data

Your computer

Encrypt Data In-Transit

End-to-End Encryption (E2EE)

Destination computer

If you ignore appropriate cybersecurity on your computing device, your data is not secure on that device

If you don't protect the recipe on your computer, a hacker can bypass the protection of E2EE

If you use end-to-end encryption, your data is secure in transit

Threat actors always attack where cybersecurity is lacking or poor

If the destination does not use appropriate cybersecurity, your data is not secure on that device

Or they can bypass the protection of E2EE on the destination computer

Securing Your Data

Anyone holding the E2EE encryption key can reveal your data by collecting a copy of your message in transit and decrypting it.

Protect Your Data in Transit

- An introduction to encryption ✓
- Communicate securely on your mobile device
- Stay safe while web surfing: Browser settings
- Stay safe while web surfing: Accessing websites securely
- Get the most out of cloud storage and services while minimizing the risk

Communicate Securely on Your Mobile Device

Use a properly vetted secure messaging app with end-to-end encryption that provides functionality for text messages and phone calls.

Place sensitive information in an encrypted file attachment when you send emails.

Source: *Protecting Your Data in Transit,* https://www.cisa.gov/resources-tools/training/how-communicate-securely-your-mobile-device, Retrieved March 18, 2025

The Problem

Text messages and voice calls are vulnerable to interception by threat actors.

5G networks provide encryption for calls and data, but carriers may downgrade 5G connections to 4G, 3G, or 2G to manage capacity, which do not offer encryption.

Traditional cell phone calls are vulnerable to interception.

Data communications that do not use encryption are vulnerable.

Source: *Protecting Your Data in Transit,* https://www.cisa.gov/resources-tools/training/how-communicate-securely-your-mobile-device, Retrieved March 18, 2025

The Problem

Email messages sent from your phone's email app or browser may be intercepted by a threat actor.

Email service providers may provide a form of encryption to protect data traveling across their own network system (Gmail to Gmail) but are unable to ensure its security when transmitted to a different email service provider.

Source: *Protecting Your Data in Transit,* https://www.cisa.gov/resources-tools/training/how-communicate-securely-your-mobile-device, Retrieved March 18, 2025

An Example of The Problem

Before December 2024, Chinese hackers penetrated the networks of U.S. and foreign telecommunications companies and gained access to systems used for court-authorized wiretaps of communications networks.

Source: *US recommends encrypted messaging as Chinese hackers linger in telecom networks, Jon Brodkin, Dec 4, 2024,* https://arstechnica.com/tech-policy/2024/12/us-recommends-encrypted-messaging-as-chinese-hackers-linger-in-telecom-networks/, Retrieved March 20, 2025

An Example of The Problem

Those Chinese hackers swept up unclassified communications from the phones of senior U.S. government officials, President-elect Donald Trump, Vice-President-elect JD Vance and the cellular records of huge swathes of Americans, putting them at risk of Chinese surveillance, too.

Source: *The White House struggles to contain massive Chinese telco hacks,* John Sakellariadis, 12/04/2024*,* https://www.politico.com/news/2024/12/04/chinese-telco-hacks-white-house-00192714, Retrieved March 20, 2025

CISA Response

"CISA strongly urges highly targeted individuals to *immediately review and apply* the best practices below to protect mobile communications. Highly targeted individuals should assume that all communications between mobile devices—including government and personal devices—and internet services are at risk of interception or manipulation."

Source: *Mobile Communications Best Practice Guidance,* https://www.cisa.gov/sites/default/files/2024-12/guidance-mobile-communications-best-practices.pdf, Retrieved March 20, 2025

The Solution

Use a secure messaging app for texting and calling on your mobile device.

Source: *Protecting Your Data in Transit,* https://www.cisa.gov/resources-tools/training/how-communicate-securely-your-mobile-device, Retrieved March 18, 2025

CISA Response – End-to-end Encryption

"Use only end-to-end encrypted communications."

"Adopt a free messaging application for secure communications that guarantees end-to-end encryption, such as Signal or similar apps. CISA recommends an end-to-end encrypted messaging app that is compatible with both iPhone and Android operating systems, allowing for text message interoperability across platforms. Such apps may also offer clients for MacOS, Windows, and Linux, and sometimes the web…"

Source: *Mobile Communications Best Practice Guidance,* https://www.cisa.gov/sites/default/files/2024-12/guidance-mobile-communications-best-practices.pdf, Retrieved March 20, 2025

CISA Response – End-to-end Encryption

"These apps typically support one-on-one text chats, group chats with up to 1,000 participants, and encrypted voice and video calls. Additionally, they may include features like disappearing messages and images, which can enhance privacy. When selecting an end-to-end encrypted messaging app, evaluate the extent to which the app and associated services collect and store metadata."

Source: *Mobile Communications Best Practice Guidance,* https://www.cisa.gov/sites/default/files/2024-12/guidance-mobile-communications-best-practices.pdf, Retrieved March 20, 2025

The CISA Position – A Summary

Use a secure messaging app that works across platforms

The app must have end-to-end encryption

The app must support text messages, including group chats

The app must support voice calls, including group calls

The app must have Multi-factor Authentication (MFA)

The app should support disappearing messages

Source: *Mobile Communications Best Practice Guidance,* https://www.cisa.gov/sites/default/files/2024-12/guidance-mobile-communications-best-practices.pdf, Retrieved March 20, 2025

Implementation of the Solution - Considerations

If you want to look at options, the United States Special Operations Command (USSOCOM) provides *Social Media Smart Cards* for guidance on how to implement privacy and security features on a number of popular communication apps at *https://www.socom.mil/documents/ussocomsocialmediasmartcards.pdf*

The guidance is for individuals at very high risk

Source: *Protecting Your Data in Transit,* https://www.cisa.gov/resources-tools/training/how-communicate-securely-your-mobile-device, Retrieved March 18, 2025

A Partial Solution

Apple’s iMessages provide end-to-end encryption only when you are communicating with other iOS users. Messages to sent to non-iOS users are not encrypted.

Similarly, Google’s Messages provide end-to-end encryption with other Google Messages users, but not with users from other services.

Source: *Protecting Your Data in Transit,* https://www.cisa.gov/resources-tools/training/how-communicate-securely-your-mobile-device, Retrieved March 18, 2025

Implementation of the Solution – CISA Recommendation

Signal is free, recommended, and an excellent choice.

Supports chats, calls, and video calls. Groups. Shares videos, GIFs, and files.

Offers disappearing messages feature. The user selects the duration.

Offers usernames. Provide a username instead of your phone number.

Offers a desktop app for Windows, Mac, and Linux/Debian users.

Offers no ads, no trackers, and is open-source.

Source: *Signal Messenger Features, https://support.signal.org/hc/en-us/sections/360001602792-Signal-Messenger-Features*, Retrieved March 20, 2025

Implementation of the Solution

The Signal website is at signal.org. The website provides

- Get Signal
- Blog
- Help
  - Getting Started
  - Features
  - Security
  - Troubleshooting
  - General

Implementation of the Solution – Privacy Policy

Signal collects:

- Phone number used to create the account
- Date of account creation
- Date account last used

Source: *Protecting Your Data in Transit,* https://www.cisa.gov/resources-tools/training/how-communicate-securely-your-mobile-device, Retrieved March 18, 2025

WhatsApp Privacy Policy

"We collect device and connection-specific information when you install, access, or use our Services. This includes information such as hardware model, operating system information, battery level, signal strength, app version, browser information, mobile network, connection information (including phone number, mobile operator or ISP), language and time zone, IP address, device operations information, and identifiers…"

Source: https://www.whatsapp.com/legal/privacy-policy

WhatsApp Privacy Policy

"We collect and use precise location information from your device with your permission when you choose to use location-related features… Even if you do not use our location-related features, we use IP addresses and other information like phone number area codes to estimate your general location (e.g., city and country)."

Source: https://www.whatsapp.com/legal/privacy-policy

Protect Your Data in Transit

- An introduction to encryption ✓
- Communicate securely on your mobile device ✓
- Stay safe while web surfing: Browser settings
- Stay safe while web surfing: Accessing websites securely
- Get the most out of cloud storage and services while minimizing the risk

Stay Safe While Web Surfing: Browser Settings - Introduction

This section identifies settings that will improve your safety while web surfing.

Use the USSOCOM's *Social Media Smart Cards* for instructions for changing the browser settings of some of the most popular browsers. The link to the instructions is *https://www.socom.mil/documents/ussocomsocialmediasmartcards.pdf*

Source: *Protecting Your Data in Transit,* https://www.cisa.gov/resources-tools/training/how-communicate-securely-your-mobile-device, Retrieved March 18, 2025

Stay Safe While Web Surfing: Browser Settings -The Problem

Threat actors often exploit vulnerabilities in web browsers to spread malware

Additionally, web browsers collect vast amounts of personal information, including interests, habits, history, and identity, which could be compromised or exposed in a data breach.

Source: *Protecting Your Data in Transit,* https://www.cisa.gov/resources-tools/training/how-communicate-securely-your-mobile-device, Retrieved March 18, 2025

Stay Safe While Web Surfing: Browser Settings -The Problem

A website may ask permission to access

- Geolocation data
- Camera
- Microphone

A website might ask permission to send pop-up notifications which can be used in phishing campaigns.

Source: *Protecting Your Data in Transit,* https://www.cisa.gov/resources-tools/training/how-communicate-securely-your-mobile-device, Retrieved March 18, 2025

Stay Safe While Web Surfing: Browser Settings -The Problem

Third-party cookies collect, store, and share information

- Website history
- Search history
- The links you clicked on
- The content you interact with on social media, and more

Data brokers and advertisers often use third-party cookies to compile and sell your information.

Source: *Protecting Your Data in Transit,* https://www.cisa.gov/resources-tools/training/how-communicate-securely-your-mobile-device, Retrieved March 18, 2025

Stay Safe While Web Surfing: Browser Settings -The Problem

Browsers themselves store data

- Browsing history
- Saved form data (personal data to autofill information)
- Location data (uses IP address, Wi-Fi, and Bluetooth
- Account credentials (if you allow the browser to store them)
- Download history (and the path to where every file is stored)
- Personal data (browsing habits and device activity)

Source: *Protecting Your Data in Transit,* https://www.cisa.gov/resources-tools/training/how-communicate-securely-your-mobile-device, Retrieved March 18, 2025

Stay Safe While Web Surfing: Browser Settings -The Solution

Protect yourself against malware

- Keep your browser up to date
- Enable automatic updates, if available
- Restart your browser regularly to allow updates to take effect

If you are accessing your browser account (Chrome, Edge, …) enable multi-factor authentication to protect your browser account.

Source: *Protecting Your Data in Transit,* https://www.cisa.gov/resources-tools/training/how-communicate-securely-your-mobile-device, Retrieved March 18, 2025

Stay Safe While Web Surfing: Browser Settings -The Solution

Manage the advertising settings in your browser to limit access to some of your browser's stored data

Turn off ad personalization

Source: *Protecting Your Data in Transit,* https://www.cisa.gov/resources-tools/training/how-communicate-securely-your-mobile-device, Retrieved March 18, 2025

Stay Safe While Web Surfing: Browser Settings -The Solution

Limit the amount of data that websites and third parties can obtain through your browser:

- Block third-party cookies in your browser settings
- Clear third-party cookies already stored (this will remove all your cookies requiring you to re-enter some information)
- Restart your browser regularly to allow updates to take effect

Source: *Protecting Your Data in Transit,* https://www.cisa.gov/resources-tools/training/how-communicate-securely-your-mobile-device, Retrieved March 18, 2025

Stay Safe While Web Surfing: Browser Settings -The Solution

Restrict site permissions as much as possible:

Do not give websites access to your location, camera, or microphone unless required for the website to function properly.

Properly vet browser extensions

Use AdBlock – recommended by CISA

Source: *Protecting Your Data in Transit,* https://www.cisa.gov/resources-tools/training/how-communicate-securely-your-mobile-device, Retrieved March 18, 2025

Protect Your Data in Transit

- An introduction to encryption ✓
- Communicate securely on your mobile device ✓
- Stay safe while web surfing: Browser settings ✓
- Stay safe while web surfing: Accessing websites securely
- Get the most out of cloud storage and services while minimizing the risk

Stay Safe While Web Surfing: Accessing Securely -The Problem

If the website's URL does not include https://, anyone with technical knowledge can view the data you share with the website.

Source: *Protecting Your Data in Transit,* https://www.cisa.gov/resources-tools/training/how-communicate-securely-your-mobile-device, Retrieved March 18, 2025

Stay Safe While Web Surfing: Accessing Securely -The Solution

Only access websites that use https://. To avoid accidental connections to http:// websites, change your preference in your browser settings to allow only HTTPS connections

Verify the website's URL by looking for slight changes from the desired URL.

Note that a threat actor can still see which website you are accessing, but they cannot see your content.

Source: *Protecting Your Data in Transit,* https://www.cisa.gov/resources-tools/training/how-communicate-securely-your-mobile-device, Retrieved March 18, 2025

Protect Your Data in Transit

- An introduction to encryption ✓
- Communicate securely on your mobile device ✓
- Stay safe while web surfing: Browser settings ✓
- Stay safe while web surfing: Accessing websites securely ✓
- Get the most out of cloud storage and services while minimizing the risk

Cloud Storage and Services – Reason to Use

You've probably lost important data while using your computer.

Cloud services enable you to back up your data and facilitate real-time collaboration with others. Examples:

- Microsoft OneDrive
- Apple iCloud,
- Google Drive
- Proton Drive

Source: *Protecting Your Data in Transit,* https://www.cisa.gov/resources-tools/training/how-communicate-securely-your-mobile-device, Retrieved March 18, 2025

Cloud Storage and Services – The Problem and Risks

Online and remote workers need a way to collaborate.

Multiple users accessing data creates an expanded attack surface. Only one person's account has to be compromised for a threat actor to access the data

Source: *Secure file sharing with Proton Drive,* https://proton.me/drive/file-sharing, Retrieved March 21, 2025

Source: *Introducing Docs in Proton Drive – Collaborative document editing that's actually private,* https://proton.me/blog/docs-proton-drive, Retrieved March 21, 2025

Cloud Storage and Services – The Solution

Use secure cloud storage and services which provide end-to-end encryption (E2EE) and use a password.

Use secure file and folder sharing. Example: Proton Drive

Use secure real-time collaboration. Example: Docs within Proton Drive

Source: *Secure file sharing with Proton Drive,* https://proton.me/drive/file-sharing, Retrieved March 21, 2025

Source: *Introducing Docs in Proton Drive – Collaborative document editing that's actually private,* https://proton.me/blog/docs-proton-drive, Retrieved March 21, 2025

Cloud Storage and Services – The Problem and Solution

There is a potential for data to be lost.

If you store your data only in the cloud and don’t save a local copy, cyber incidents such as a denial-of-service attack could lead to the temporary or even permanent loss of your data.

Source: *Protecting Your Data in Transit,* https://www.cisa.gov/resources-tools/training/how-communicate-securely-your-mobile-device, Retrieved March 18, 2025

Cloud Storage and Services – The Problem and Risks

Less control over your data. Your data is stored on servers you do not control. If the servers are located in another country, that country may require the cloud service to disclose your data.

Note that the service can be compelled to disclose your data only if the service holds the encryption keys.

.

Another risk: scheduled server maintenance may prevent access to your data.

Source: *Protecting Your Data in Transit,* https://www.cisa.gov/resources-tools/training/how-communicate-securely-your-mobile-device, Retrieved March 18, 2025

Cloud Storage and Services – Risks to Data at Rest

If the cloud service has the end-to-end encryption key, your data at rest could be read by the service:

Microsoft OneDrive
Google Drive and Docs
Apple Standard Data Protection for iCloud.

Your data at rest is not readable by a service if you hold the encryption keys:

Apple Advanced Data Protection for iCloud
Any Proton product: Drive, Docs, Email, etc.

Cloud Storage and Services

The below Sources are for the *Risks to Data at Rest* slide

Source: *Proton Key Transparency Whitepaper,* https://proton.me/files/proton_keytransparency_whitepaper.pdf, Retrieved March 21, 2025

Source: *Key management,* https://proton.me/support/pgp-key-management, Retrieved March 21, 2025

Source: *Encryption and key management overview,* https://learn.microsoft.com/en-us/compliance/assurance/assurance-encryption, Retrieved March 21, 2025

Source: *iCloud data security overview,* https://support.apple.com/en-us/102651, Retrieved March 21, 2025

Source: *Default encryption at rest,* https://cloud.google.com/docs/security/encryption/default-encryption, Retrieved March 21, 2025

Cloud Storage and Services – The Risks and Solution

Ensure that these services encrypt your data and are headquartered in a country with privacy and security laws that help protect your data.

Proton is in Switzerland which has strict privacy and security laws.

Source: *Protecting Your Data in Transit,* https://www.cisa.gov/resources-tools/training/how-communicate-securely-your-mobile-device, Retrieved March 18, 2025

Cloud Storage and Services – An Example of Risks

The UK recently issued a secret order to Apple, requiring the creation of a backdoor in their encryption that would enable the UK to access the encrypted data of any Apple user worldwide.

Source: *UK demands Apple break encryption to allow gov't spying worldwide, reports say,* Jon Brodkin https://arstechnica.com/tech-policy/2025/02/uk-demands-apple-break-encryption-to-allow-govt-spying-worldwide-reports-say, February 7, 2025

Cloud Storage and Services – An Example of Risks

Apple responded by discontinuing Advanced Data Protection (ADP) in the UK. The user holds the encryption keys when using ADP.

Instead, new UK users will have available only Standard Data Protection (SDP). Apple holds the encryption keys when using SDP.

Current UK users of Advanced Data Protection will soon have to downgrade to Standard Data Protection.

Source: *Apple can no longer offer Advanced Data Protection in the United Kingdom to new users,* https://support.apple.com/en-us/122234, Retrieved March 24, 2025

Standard Data Protection Encryption

Standard Data Protection does not provide end-to-end encryption for these categories:

- iCloud Backup
- iCloud Drive
- Photos
- Notes
- Reminders
- Safari Bookmarks
- Siri Shortcuts
- Voice Memos
- Wallet Passes
- Freeform

Source: *Apple can no longer offer Advanced Data Protection in the United Kingdom to new users,* https://support.apple.com/en-us/122234, Retrieved March 24, 2025

Protect Your Data in Transit

- An introduction to encryption ✓
- Communicate securely on your mobile device ✓
- Stay safe while web surfing: Browser settings ✓
- Stay safe while web surfing: Accessing websites securely ✓
- Get the most out of cloud storage and services while minimizing the risk ✓

Summary

Use messaging apps where you hold the encryption keys, allowing you to protect your information.

Change browser settings to protect your information.

Select cloud storage and services that allow you to hold the encryption keys.

Securing Your Home

April 8, Tuesday, 10 am

Cultural Center Education Room

Thank You,
Bill Skelly

Articles

For the latest cybersecurity information, these are accurate and reliable sources:

Ars Technica	arstechnica.com
Bleeping Computer	bleepingcomputer.com
CISA	cisa.gov
Forbes	forbes.com
Proton Blog	proton.me/blog
Proton VPN Blog	protonvpn.com/blog

Books

Beginner's Introduction to Privacy, Naomi Brockwell, (Independently Published, 2023)

Means of Control: How the Hidden Alliance of Tech and Government is Creating a New American Surveillance State, Bryon Tau, (Crown, 2024)

Your Face Belongs to Us: A Tale of AI, A Secretive Startup, and the End of Privacy, Kashmir Hill, (Crown, 2024)

Extreme Privacy: What It Takes To Disappear, 5th Edition, Michael Bazzell, (Independently Published, 2024)

Firewalls Don't Stop Dragons, 5th Edition, Carey Parker, (Apress, 2024)

YouTube Channels

David Bombal, [Cybersecurity, Privacy, IT] https://www.youtube.com/@davidbombal

Naomi Brockwell TV, [Privacy]
https://www.youtube.com/channel/UCSuHzQ3GrHSzoBbwrIq3LLA

PC Security Channel, [Cybersecurity, Malware]
https://www.youtube.com/channel/UCKGe7fZ_S788Jaspxg-_5Sg

Questions?