Willow Valley Computer Club

Member of apcug

An International Association of Technology & Computer User Groups

Project Upskill II

Protecting Your Accounts from Compromise

Al Williams

October 8, 2025

What Did the Do You Really Know Session Do for You?

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

Privacy Policies of the apps and web pages you're using reveal 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.

What Did the Basic Cybersecurity Session Do For You?

I showed you how to make it much harder for hackers to get into your laptop, desktop, or smartphone by:

- Vetting technologies before using them
- Keeping your operating system and apps up to date
- Ensuring antivirus and malware protections are active
- Protecting the physical security of your devices
- Implementing User Account Control to protect your PC
- Managing application permissions for privacy and security

What Will This Session Do For You?

I’m going to show you best practices for protecting your accounts.

Threat actors develop new attacks and developers react. It’s a continuous cycle.

How-to information is at the bottom of the slides.

The Account Compromise Concerns

- 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

Many highly reputable companies
say it is just a matter of time
before they suffer a data breach

You can put in practice these
Account Compromise Concerns
to minimize the resulting damage

There are three ways your passwords and PIN codes
can be found by threat actors
when you’re using a website

Finding Passwords and PIN Codes

- Threat actors may find your password or PIN code by trial and error using a list of common passwords
- Threat actors may use rainbow tables to find your password or PIN code
- Threat actors may use brute force to find your password or PIN code

How do Websites Use Passwords?

- They may store each password as plain text (meaning that you can read it like reading a page)

Finding Passwords and PIN Codes

- Threat actors may find your password or PIN code by trial and error using a list of common passwords

Lists of Common Passwords and PIN Codes

- 14,658,515,294 accounts have been exposed in data breaches
- Humans tend to be predictable. Research shows that most people use 1 of 10,000 common passwords
- These passwords are up to 18 characters long
- Those passwords are available in a file named rockyou.txt, created in 2009, that contains over 14 million plaintext passwords
- The longest password in rockyou.txt is 285 characters

Number of Accounts Source: *haveibeenpwned?,* https://haveibeenpwned.com, Retrieved 2/20/2025

Lists of Common Passwords and PIN Codes

123456
12345
123456789
password
iloveyou
princess
1234567
rockyou
12345678
abc123

The ten most popular passwords

Source: *rockyou.txt,* https://github.com/zacheller/rockyou, Retrieved 2/20/2025

Lists of Common Passwords and PIN Codes

- rockyou2024.txt has almost 10 billion passwords

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	Instantly	Instantly	Instantly
8	Instantly	Instantly	Instantly	Instantly	Instantly
9	Instantly	Instantly	Instantly	Instantly	Instantly
10	Instantly	Instantly	Instantly	Instantly	Instantly
11	Instantly	Instantly	Instantly	Instantly	Instantly
12	Instantly	Instantly	Instantly	Instantly	Instantly
13	Instantly	Instantly	Instantly	Instantly	Instantly
14	Instantly	Instantly	Instantly	Instantly	Instantly
15	Instantly	Instantly	Instantly	Instantly	Instantly
16	Instantly	Instantly	Instantly	Instantly	Instantly
17	Instantly	Instantly	Instantly	Instantly	Instantly
18	Instantly	Instantly	Instantly	Instantly	Instantly

Password table if your password has been previously stolen, uses dictionary words, or if you reuse it between websites.

Source: *https://www.hivesystems.com/blog/are-your-passwords-in-the-green*, Retrieved 2/20/2025

How do Websites Use Passwords?

- They may calculate a hash of the password and store the hash so that no one can read the password even if the website suffers a data breach

Storing a Password as a Hash

- A hash is a one-way mathematical function that takes a password of any length and generates a fixed-length string of characters
  - BigCat47Low -> 58922334
  - 1234 -> 89762940
- A hash of a unique password will always generate the same string of characters – it's repeatable
- When you enter your password on a website, the password is entered into the website's hash function.
- That hash is compared to the hash stored on the website when you created the account. If it matches, you are logged into the website.

Storing a PIN Code as a Hash

- When you create a PIN Code on a device, the PIN Code is entered into the device's hash function and stored on the device.
- The next time you log in, you enter the PIN Code. A hash is calculated and compared to the hash stored on the device when you created the account. If it matches, you are logged into the device.

Using Rainbow Tables

- A rainbow table is a precomputed list of passwords and the corresponding hash for each password
- The threat actor finds the hashed password in the data breach and looks up the corresponding password in the rainbow table

How do Websites Use Passwords?

- They may create a salted hash to prevent the use of rainbow tables

What is a Salted Hash

- A salted hash adds a string of characters to your password before computing the hash
- The salt is kept a secret – otherwise, hackers could easily create a rainbow table using the salt

Finding Passwords and PIN Codes

- Threat actors may use brute force to find your password or PIN code

If you reuse a password or use a password in tables such as rockyou.txt, then the time to brute your password is shorter.

Source: *www.hivesystems.com/password*, Retrieved 2/20/2025

TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2024

How did we make this? Learn at hivesystems.com/password

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	3 secs	6 secs	9 secs
5	Instantly	4 secs	2 mins	6 mins	10 mins
6	Instantly	2 mins	2 hours	6 hours	12 hours
7	4 secs	50 mins	4 days	2 weeks	1 month
8	37 secs	22 hours	8 months	3 years	7 years
9	6 mins	3 weeks	33 years	161 years	479 years
10	1 hour	2 years	1k years	9k years	33k years
11	10 hours	44 years	89k years	618k years	2m years
12	4 days	1k years	4m years	38m years	164m years
13	1 month	29k years	241m years	2bn years	11bn years
14	1 year	766k years	12bn years	147bn years	805bn years
15	12 years	19m years	652bn years	9tn years	56tn years
16	119 years	517m years	33tn years	566tn years	3qd years
17	1k years	13bn years	1qd years	35qd years	276qd years
18	11k years	350bn years	91qd years	2qn years	19qn years

HIVE SYSTEMS

› Hardware: 12 x RTX 4090 | Password hash: bcrypt

If a threat actor wants to brute force your password, they can use significant computing power.

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols	Hardware
8	2 hours	4 months	92 years	375 years	989 years	RTX 2080
8	17 mins	4 weeks	18 years	72 years	189 years	RTX 3090
8	9 mins	2 weeks	9 years	38 years	99 years	RTX 4090
8	2 mins	2 days	2 years	7 years	17 years	A100 x8
8	1 min	2 days	1 year	4 years	12 years	A100 x12
8	Instantly	3 mins	11 hours	2 days	5 days	A100 x10,000 (ChatGPT)

Max time required to crack randomly generated 8-character bcrypt password hashes set to 32 iterations of various complexity on different hardware.

Source: *https://www.hivesystems.com/blog/are-your-passwords-in-the-green*, Retrieved 2/20/2025

Finding Passwords and PIN Codes

- Since it takes a month to 164 million years to brute force passwords with 7 to 12 characters, using 12 high performance graphics cards, a threat actor might try using a password list like rockyou.txt first

Formulate Strong Password and PIN Codes

- Weak passwords are the primary cause of account security breaches
- Use a strong password to keep threat actors from stealing your information
- Use at least 16 characters with a mix of upper case, lower case, numbers, and symbols
- Or, use 4 to 7 unrelated words with at least one number and symbol to create a passphrase
- Use a unique password or passphrase for every account
- PIN codes should also be long, random, and unique (avoid the 123456 pattern)

Source: *Formulate Strong Passwords and PIN Codes*, https://www.cisa.gov/resources-tools/training/formulate-strong-passwords-and-pin-codes, Retrieved 2/20/2025

Formulate Strong Password and PIN Codes

- Why 16 characters? It takes hundreds of years to brute force 9 characters.
- Because the techniques to brute force passwords are constantly improving.
- You won’t know that 9 characters can be hacked.
- 16 characters provide future-proof safety.

Finding Passwords and PIN Codes

- Threat actors may find your password or PIN code by trial and error using a list of common passwords ✓
- Threat actors may use rainbow tables to find your password or PIN code ✓
- Threat actors may use brute force to find your password or PIN code ✓

Account Compromise Concerns

- 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

Use a Password Manager

- It is difficult, if not impossible, to remember passwords with 16 characters or more, or 4 to 7-word passphrases
- You'll likely need these passwords / passphrases for multiple accounts
- Password managers are designed to solve the problem of having and remembering these long passwords and passphrases

Source: *Cyb3R_Sm@rT!: Use a Password Manager to Create and "Remember" Strong Passwords*, https://www.cisa.gov/resources-tools/training/cyb3rsmrt-use-password-manager-create-and-remember-strong-passwords, Retrieved 2/21/2025

Use a Password Manager

- Password managers can generate random passwords and passphrases
- Password managers can be cloud-based so that you can share your password vault (all the information in the password manager) across all your devices
  - The Computer Club recommends Bitwarden for this application
  - An alternate is 1Password – but it isn't open source

Source: *Cyb3R_Sm@rT!: Use a Password Manager to Create and "Remember" Strong Passwords*, https://www.cisa.gov/resources-tools/training/cyb3rsmrt-use-password-manager-create-and-remember-strong-passwords, Retrieved 2/21/2025

Use a Password Manager

- Or, use a password manager whose vault is locally stored on your computer – you can store it on a USB drive - it won't sync to any other computer
  - The Computer Club recommends KeePassXC for this application
- Backups are critical
  - Save to a USB drive (thumb drive, flash drive) - recommended
  - Make a paper backup
  - Export as an HTML file – need to encrypt the file
  - Upload to cloud storage – need to encrypt the file
- Bitwarden backups discussion soon

Use a Password Manager

- The master password gives you access to the password manager.
- The master password should be memorized, and a written copy should be kept in a secure location, such as a safe

Source: *Cyb3R_Sm@rT!: Use a Password Manager to Create and "Remember" Strong Passwords*, https://www.cisa.gov/resources-tools/training/cyb3rsmrt-use-password-manager-create-and-remember-strong-passwords, Retrieved 2/21/2025

Use a Password Manager

- For each new account, create a random password or passphrase using the password manager's generator

Source: *Cyb3R_Sm@rT!: Use a Password Manager to Create and "Remember" Strong Passwords*, https://www.cisa.gov/resources-tools/training/cyb3rsmrt-use-password-manager-create-and-remember-strong-passwords, Retrieved 2/21/2025

Use a Password Manager

- For each account, store this information in the password manager:
  - Username
  - Password or passphrase
  - What authenticator you are using with the account, if any
  - Any account recovery information you provided when you created the account or the account provided you (recovery code)
    - Email
    - Phone number
    - Recovery code

Source: *Cyb3R_Sm@rT!: Use a Password Manager to Create and "Remember" Strong Passwords*, https://www.cisa.gov/resources-tools/training/cyb3rsmrt-use-password-manager-create-and-remember-strong-passwords, Retrieved 2/21/2025

To Recover Access to the Password Manager

- Make encrypted backups of the contents of the password manager vault
- Bitwarden
  - Export the vault as an encrypted .json file
  - The password for the file must be remembered.
  - I suggest the password be the same as the master password

To Recover Access to the Password Manager

- Emergency Sheet – paper only – store in a safe location – for you and your family
  - The name of the password manager
  - The server the password manager is using (for Bitwarden, it is .com or .de)
  - The username to log into the password manager
  - The master password
  - The authenticator being used for multi-factor authentication access to the password manager. Using MFA to access your password manager is recommended.
  - Any recovery codes the password manager provided during account creation to regain access.

Bitwarden – Password Strength Testing

Bitwarden offers a password strength testing tool

Describes password strength and estimated time to crack the password

You don’t need to put in your password. You can put in a password similar to yours.

Website: https://bitwarden.com/password-strength/

Source: https://bitwarden.com/password-strength/

Account Compromise Concerns

- 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

Why a Strong Password Isn’t Enough

- Threat actors have many methods for gaining unauthorized access to accounts protected by one form of authentication, such as your username and password
- Phishing is one common method that threat actors use to steal account credentials – to get you to think you’re entering username and password, personally identifiable information, or credit card information into a legitimate website or document
- The solution is to use Multi-Factor Authentication (MFA) in addition to your password

Types of MFA

- Something you know – a password, PIN code, or security question
- Something you have – a software token, physical token, one-time password, authenticator, hardware security key
- Something you are – biometric data such as FaceID or TouchID

Ranking of MFA from Strongest to Weakest

- Physical tokens with FIDO authentication – Yubico security keys
- Physical token examples without FIDO authentication
  - USB tokens
  - Smart cards

Ranking of MFA from Strongest to Weakest

- Software token examples
  - Bitwarden Authenticator – within Bitwarden (cross-platform) or a stand-alone app (iPhone and Android)
  - Authy Authenticator (iPhone and Android)
  - KeePassXC Authenticator (Windows, macOS, Linux)
  - Microsoft Authenticator (iPhone and Android)
- Note: Multiple authenticators may be used. They'll show the same code.
- Biometric authentication such as FaceID and TouchID
- Email one-time passcode
- SMS one-time passcode

Account Compromise Concerns

- 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

Why Passkeys are a Good Thing

- Phishing resistant – passkeys cannot be fooled by threat actors
- Secret information, such as passwords, is never transmitted over the Internet (Note that the information is encrypted during transmission)
- Passkeys are always strong (like strong passwords)
- Typically, logins are done with a fingerprint, face scan or a PIN to authenticate
- You don’t have to remember passwords for each website.
- You can sync passkeys across your devices if they are stored in a cross-platform password manager such as Bitwarden

Account Compromise Concerns

- 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

Why Email Aliases are a Good Thing

- Protect your primary email address
  - Using an alias helps protect your actual email address from spam, marketing emails, and potential data breaches
  - Use a separate email alias for each new account to thwart threat actors who try to use the email address as your identity in a data breach to access other accounts
- Spam prevention
  - If an account starts sending excessive spam, delete the email alias, which also isolates the account and prevents phishing attempts using that email alias

Why Email Aliases are a Good Thing

- When creating a new account, use an email alias
- The website knows only your email alias, it does not know your real email address
- An email alias protects your primary email address
- Sample email aliases:
  - xxxx.1234@passmail.net – Proton
  - stungbullish587@simplelogin.com - SimpleLogin
- Recommended sources
  - Proton.me
  - SimpleLogin.com

Why Email Aliases are a Good Thing

- SimpleLogin is a recommended email alias provider
  - Free account provides 10 aliases
  - Premium account provides unlimited aliases
- The Proton Unlimited plan includes the premium SimpleLogin features

Account Compromise Concerns

- 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

Some Browser Extensions are a Bad Thing

- Because multi-factor authentication (MFA) is so effective, threat actors are looking for ways to bypass MFA
- If they can successfully phish someone, they may use their access to install a malicious extension in their browser
- This type of extension captures usernames and passwords as the user logs into the website
- If you see an extension in your browser that you did not install, treat it as suspicious
- This attack does not work if the user is using passkeys

Account Compromise Concerns

- 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 ✓

Protecting Data Stored on Your Devices

October 15, Wednesday, 10 am

Cultural Center Education Room

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?