How to be Safe in an Online World

Workshop Objectives

- Understand common security threats
- Learn privacy best practices
- Implement security tools and techniques
- Develop a personal security strategy

MISSION: STRONGHOLD

Agenda

1. Current Threat Landscape
2. Password Security
3. Two-Factor Authentication
4. Browser Security & Privacy
5. Network Security
6. Privacy Tools
7. Physical Security
8. Keeping Children Safe Online
9. Best Practices

You Can Do this

Take Small Steps

Practice Skepticism

> *If it sounds to good to be true it probably is*

~ Everyone's grandma

No one has more incentive to protect you than you.

> *Convenience is the enemy of security*

~ Steve Gibson - Programmer and Security Expert

> *There are no solutions, only trade-offs.*

~ Thomas Sowell

Current Threat Landscape

Top Security Threats

- **Phishing attacks** - 80% of breaches involve phishing
- **Ransomware** - Growing threat to individuals and organizations
- **Data breaches** - Personal data exposure
- **Social engineering** - Manipulation tactics
- **Zero-day exploits** - Unknown vulnerabilities

Privacy Concerns

- **Data collection** by websites and apps
- **Tracking** across the internet
- **Third-party data sharing**
- **Government surveillance**

Identity Theft

What is it?

- Criminals use your personal information to:
  - Open credit accounts
  - File fraudulent tax returns
  - Make purchases
  - Access medical services

Identity Theft

Red flags:

- Unfamiliar accounts on credit report
- Denied credit unexpectedly
- Medical bills for services you didn't receive
- Missing mail or unexpected bills

Protecting Against Identity Theft

Credit Freezes (Most Effective):

- Free at all three credit bureaus
- Prevents new accounts from being opened
- Must freeze at: Equifax, Experian, TransUnion
- Lift temporarily when you need credit

Identity Theft Prevention Strategies

1. **Secure your Social Security Number**
   - Never carry SSN card in wallet
   - Only provide when legally required
   - Ask why it's needed before giving it out

Identity Theft Prevention Strategies

2. **Protect your mail**
   - Use locked mailbox or P.O. box
   - Sign up for Informed Delivery (USPS)
   - Shred sensitive documents

Identity Theft Prevention Strategies

3. **Monitor financial accounts**
    - Enable transaction alerts
    - Review statements monthly

If it happens: File report at IdentityTheft.gov immediately

MISSION: STRONGHOLD

Password Security

Password Problems

Common mistakes:

- Using the same password everywhere
- Simple, easy-to-guess passwords
- Storing passwords insecurely
- Never changing passwords after breaches

Password Best Practices

1. **Use a password manager** (Bitwarden, 1Password, ProtonPass)
2. **Create strong, unique passwords** for each account
3. **Enable breach monitoring**
4. **Change passwords** after known breaches

MISSION: STRONGHOLD

Password Managers

Why Password Managers?

- Create strong passwords
- Only need to remember one password
- Fill in your info (no more passwords on paper)
- Data is encrypted with a strong master password
- Accessible from all your devices

Creating Strong Passwords with Mnemonics

The Method: Take a memorable sentence and use the first letter of each word, plus numbers and symbols.

Mnemonic Example

John 3:16:

> *"For God so loved the world that He gave His only Son"*

Becomes: `Fgsltw,tHgHos!` Or `FgsLtwTHgHos316!`

Why this works:

- ✅ Meets length requirements (12-16+ characters)
- ✅ Includes uppercase, lowercase, numbers, symbols
- ✅ Easy to remember (you know the phrase)
- ✅ Hard to crack
- ✅ Unique to you

Two-Factor Authentication (2FA)

Why 2FA Matters

2FA reduces account compromise by 99.9%

Even if your password is stolen, attackers need:

- Something you know (password)
- Something you have (phone, security key)

2FA Methods

From **least** to **most** secure:

1. SMS codes (better than nothing)
2. Authenticator apps (Bitwarden)
3. Hardware security keys (YubiKey)
4. Biometric authentication (Finger print / face)

Setting Up 2FA

Recommended apps:

- Bitwarden (integrated)
- Aegis (Android only)
- 1Password (integrated)
- Authy (cloud backup)

Always save backup codes!

2FA Minimum

- Financial
- Email

Browser Security & Privacy

Privacy is Not Secrecy

Privacy is simply choosing who you share information with.

Browser Choice Matters

Privacy-focused browsers:

- Brave (built-in blocking)
- Mullvad Browser

Network Security

Public Wi-Fi Dangers

Never do these on public Wi-Fi:

- Banking or financial transactions
- Entering passwords (without VPN)
- Accessing sensitive data

Always:

- Use a VPN
- Verify network name with staff
- Use HTTPS sites only

VPN Basics

What a VPN does:

- Encrypts your internet traffic
- Hides your IP address
- Bypasses geographic restrictions

MISSION: STRONGHOLD

How a VPN Works

WITHOUT VPN:

```
You ──────────> ISP ─────────────> Website
        │                    │
        └─ ISP can see:      └─ Website can see:
           - What sites        - Your real IP
           - Your data         - Your location
           - Your activity     - Your behavior on their site
                               - Browser fingerprint
```

WITH VPN:

```
You ──────────> ISP ──────────────> VPN Server ─────────> Website
        │                      │                    │
        └─ ISP can only see:   └─ VPN Forwards      └─ Website can see:
           - Encrypted            encrypted            - VPN's IP (not yours)
             tunnel to VPN        traffic to           - VPN's location (not yours)
           - Can't see            website              - Your behavior on their site
             destination                               - Browser fingerprint
```

Key Point: VPN server can see everything your ISP used to see

VPNs are NOT magic security tools:

❌ Does NOT make you anonymous

❌ Does NOT protect from malware/viruses

❌ Does NOT hide everything

❌ Does NOT secure unencrypted connections

Recommended VPNs

Trustworthy providers:

- **Mullvad** - Anonymous, no logs, Audited, accepts cash
- **IVPN** - Audited, transparent, no logs
- **ProtonVPN** - Swiss privacy laws, open source

Privacy Tools

Understanding Email

Issues with Email:

- It is essentially a digital postcard
- It is a gateway into most of your accounts
- Usually not encrypted on the server
- Use it responsibly by knowing the risks
- Phishing and viruses

Email Privacy

Issues with Gmail/Outlook:

- Email scanning for ads
- Data mining
- Privacy policy changes

Email Privacy

Private alternatives:

- ProtonMail (encrypted)
- Tutanota (encrypted)
- Fastmail (privacy-focused)

General Email Safety Tips

- Don't click links
- Check the sender's email address
- Confirm things outside of the email

Search Engines

Google alternatives:

- Brave Search (no tracking, own index)
- DuckDuckGo (no tracking, Bing results)
- Startpage (anonymized Google results)

Messaging Security

Secure messaging apps:

App	End-to-End Encrypted	Metadata Protection
Signal	✅	✅
WhatsApp	✅	❌
Telegram	⚠️ (Secret chats only)	❌
iMessage	✅	⚠️

Recommendation: Signal

People Search / Data Brokers

- Data brokers compile public records
- Social media oversharing
- Leaked databases

Remove yourself from data brokers

- Services like EasyOptOuts, DeleteMe, (paid)
- Manual removal (time-consuming but free)
- Check: WhitePages, Spokeo, BeenVerified, PeopleFinder

Physical Security

Device Lock Security

Use strong PINs/passwords:

- **Phones & tablets:** 6+ digit PIN or strong password
- **Computers:** Strong password (not just PIN)
- Avoid: simple patterns (1234, 0000), birthdays, sequential numbers

Device Lock Security

Auto-lock settings:

- Set devices to lock after 1-2 minutes of inactivity
- Shorter timeout = more security, less convenience
- Balance based on your risk tolerance

Biometric Authentication Trade-offs

Face ID / Face Recognition:

- ✅ Convenient and fast
- ✅ Harder to shoulder-surf
- ❌ Can be unlocked while you're sleeping/unconscious
- ❌ May unlock with photos/masks (varies by quality)
- ❌ Can be compelled by law enforcement (in some jurisdictions)

Biometric Authentication Trade-offs

Fingerprint / Touch ID:

- ✅ Quick and convenient
- ✅ Works when face is covered
- ❌ Can be lifted from surfaces
- ❌ Can be compelled by law enforcement (in some jurisdictions)
- ❌ Doesn't work with wet/dirty fingers

Biometric Authentication Trade-offs

PIN/Password:

- ✅ Can't be taken from you physically
- ✅ Legal protections in some jurisdictions (5th Amendment)
- ❌ Can be shoulder-surfed
- ❌ Less convenient to type frequently

Best practice:

Use biometrics for convenience, but know how to quickly disable them (e.g., iPhone: press power button 5 times)

USB Data Blockers

What they do:

- Prevent "juice jacking" at public charging stations
- Block data transfer pins, allow only power
- Protect against malicious charging cables

When to use:

- Airports, hotels, conferences
- Any public USB charging port
- Untrusted charging stations

Cost: $5-15 **Brands:** PortaPow, Syncstop

Camera Protection

Why they matter:

- Malware can activate cameras/mics remotely
- Smart assistants are always listening
- Video conferencing apps can have vulnerabilities
- School IT staff have been caught spying on students

Camera Protection

Webcam Covers:

- Physical slider covers for laptop/desktop cameras
- Adhesive covers for phone cameras
- Prevents unauthorized surveillance
- **Cost:** $5-10

Privacy Screens

What they are:

- Thin filters that attach to your screen
- Narrow viewing angle (typically 60°)
- Screen appears black from the side

Privacy Screens

Benefits:

- Prevents shoulder surfing in public
- Protects sensitive data on planes, trains, coffee shops
- Works with laptops, tablets, monitors, phones

Cost: $20-40 depending on screen size

RFID Blocking

What is RFID?

- Radio Frequency Identification
- Contactless credit cards, passports, ID badges
- Can be read from several feet away

RFID Blocking

Threats:

- Digital pickpocketing
- Passport data theft
- Credit card skimming

RFID Blocking

RFID Blocking Products:

- **Wallets/card sleeves** - Block card readers ($10-30)
- **Passport holders** - Protect passport chips ($10-20)
- **Badge holders** - Secure work ID badges ($5-15)

MISSION: STRONGHOLD

Keeping Children Safe Online

Online Risks for Children

Major concerns:

- **Online predators** - Grooming, manipulation
- **Inappropriate content** - Violence, pornography
- **Cyberbullying** - Harassment, exclusion, threats
- **Oversharing** - Privacy violations, future consequences
- **Gaming risks** - In-game chat, scams, addiction
- **Social media pressure** - Mental health impacts

Parental Controls & Monitoring

Device-level controls:

- Screen time limits (iOS Screen Time, Android Digital Wellbeing)
- Content filters and age restrictions
- App installation permissions
- Location sharing (for safety)

Parental Controls & Monitoring

Router-level controls:

- DNS-based content filtering
- Time-based access controls
- Block specific websites

Parental Controls & Monitoring

DNS Filtering Options:

- **Cloudflare Family DNS**
  - Blocks malware + adult content
  - Fast, private, and free
  - Set on router to protect whole network
- **OpenDNS Family Shield**

Note: Virtually no downside to DNS filtering

MISSION: STRONGHOLD

Parental Controls & Monitoring

Monitoring tools:

- CovenantEyes - monitors content filtering
- Bark - monitors texts, social media

Balance: Monitoring should decrease as trust and maturity increase

When to Give a Smartphone

It's okay to wait:

- No "right age" - depends on maturity and need
- Many experts recommend waiting until 13-14+
- Peer pressure is real, but you know your child best
- Delaying can reduce exposure to risks
- **Easier to give privileges than take them away later**

MISSION:
STRONGHOLD

Alternatives to smartphones:

- **Feature phones** (basic phones with calls/texts only)
  - Light Phone, or basic flip phones
  - Communication without internet/apps/social media
- **Smartwatches with GPS** (e.g., Gizmo Watch, Apple Watch SE)
  - Can call/text parent only
  - Location tracking for safety
- **Locked-down smartphones**
  - Use parental controls to disable app store
  - Whitelist only parent contact and emergency services
  - Gradually add features as they mature

Physical Environment & Habits

Device storage overnight:

- Designate a central charging location outside bedrooms
- All devices (phones, tablets, laptops) go there at bedtime
- Reduces nighttime usage and sleep disruption
- Parents can check devices if needed

Physical Environment & Habits

Computer placement:

- Keep computers in common areas (living room, kitchen)
- Avoid bedrooms or secluded spaces
- Angle screens so they're visible to others passing by
- Creates natural accountability and supervision

Communication Strategies

Build trust:

- React calmly to mistakes
- Focus on teaching, not just punishing
- Share your own online experiences
- Make yourself the "safe person" to tell

Resources for parents

- Common Sense Media - age-based reviews
- ConnectSafely.org - tips for popular platforms

Best Practices

Getting Started: Priority Actions

Feeling overwhelmed? Start here:

Week 1 - Critical basics:

- ✅ Set up password manager + create strong master password
- ✅ Enable 2FA on email and financial accounts
- ✅ Enable automatic software updates
- ✅ Set device auto-lock to 1-2 minutes

Week 2-3 - Protection:

- ✅ Freeze your credit at all three bureaus
- ✅ Review and minimize browser extensions

Month 2 - Privacy:

- ✅ Remove yourself from data broker sites
- ✅ Set up VPN for public WiFi use

Ongoing:

- Check credit reports quarterly
- Update passwords after breaches

Resources

Recommended Apps/Services

- Password manager - bitwarden.com
- 2FA - Bitwarden.com
- VPN - Mullvad.net
- Browser - Brave.com
- Search - search.brave.com
- Email - proton.me/mail
- Messaging - signal.org
- Data removal - easyoptouts.com

Questions?

- Email: [info@missionstronghold.org]
- Workshop Materials: [missionstronghold.org/security2025]

Thank You!

Remember:

Security is a journey, not a destination

"Security is not a product, but a process" - Bruce Schneier