

Protecting Your Privacy

In the Digital Age

Simple Steps, Big Impact

Elbert T Chester, Forensic CPA



The Digital Privacy Crisis

61% of Americans have had personal data breached

44% have experienced multiple breaches

- Billions of data points collected and exploited daily

Identity theft costs victims **\$14,000+** on average

- Cyberattacks affect individuals, businesses, and organizations globally

Your data is valuable—protect it.



Learning Objectives

Identify what personal information is targeted and collected

Understand importance of privacy and related risks/threats

Recognize various types of scams used to obtain personal info

Learn techniques, technologies, and settings to protect privacy

Master social media risks and best practices



What Information Is Collected?

Your Digital Footprint Is Larger Than You Think

- IP Address & Device Information
- Name, Email, Phone Number
- Home Address & Location Data
- Social Security Number & Finances
- Browsing History & Search Queries
- Purchase History
- Biometric Data
- Family Names & Pet Names
- Work History
- Birthdays & Personal Dates

Every interaction creates data trails.



Why Personal Privacy Matters

1. Protection from Identity Theft

Safeguards against unauthorized access and reduces fraud risk

2. Maintaining Confidentiality

Ensures confidentiality of communications and fosters trust

3. Preserving Autonomy

Empowers you to control dissemination of your personal data

4. Personal Safety

Ensures physical safety and prevents location-based attacks



Online Threats & Risks

Phishing Attacks

Deceptive emails trick you into revealing sensitive information

Data Breaches

Expose personal info leading to identity theft and fraud

Cyberstalking

Use of platforms to harass and invade privacy



Four Major Scam Categories

Financial Scams

Advanced fees, debt management, credit cards, cryptocurrency, tax fraud

Imposter Scams

Romance, job offers, charity, government, tech support

Hacked Accounts

Ransomware, malware, phishing, email compromise

Identity Theft

Criminal, financial, medical, social media, Social Security



Recognizing Phishing Scams

Three Defense Strategies:

1. **Be Cautious with Links** – Never click suspicious links in emails, websites, or pop-ups
2. **Verify the Source** – Check email addresses and look for spelling/formatting errors
3. **Keep Info Private** – Never share passwords or financial details with unknown sources

Red Flags:

- Emails from "support@company.offers.com" (not official domain)
- Urgent action required language
- Too good to be true offers
- Grammar and spelling errors



Strong Passwords: Do's and Don'ts

✓ DO's

- Use 12-15+ characters minimum
- Mix letters, numbers, symbols
- Different passwords for each account
- Use a password manager
- Change passwords regularly

✗ DON'Ts

- Personal names or dates
- Pet names and birthdays
- Write passwords down
- Share with anyone
- Same password everywhere



Password Managers

Making Strong Passwords Easy

- Store all passwords securely
- Remember only ONE master password
- Enable extremely complex passwords
- Apps, browser extensions, website access
- Independently audited for security

Recommended Options:

1Password • Bitwarden • Dashlane • NordPass



Multi-Factor Authentication (2FA)

Extra Locks on Your Digital Door

Requires 2+ authentication steps • Dramatically reduces unauthorized access • Works even if password is compromised

Common Methods:

- Authenticator Apps (Google, Microsoft, Authy, 2FAS)
- SMS/Text Message Verification
- Fingerprint Scanners

Set up 2FA on critical accounts first, then expand to all accounts



Regular Updates & VPNs

Software Updates

- Phone OS (Android/iOS)
- All apps and software
- Bug fixes & security patches
- Protect against vulnerabilities

VPNs

- Mask identity & IP address
- Encrypt online activities
- Essential for public Wi-Fi
- ExpressVPN, NordVPN, IPVanish



Privacy-Focused Tools

Privacy Browsers:

Brave, DuckDuckGo, Firefox, LibreWolf, Epic, Ghostery, Avast

Encrypted Messaging:

Signal, Telegram, WhatsApp

App Access Control:

- Only grant necessary permissions
- Regularly revoke unused app access
- More access = More data sharing
- Trust is essential



Social Media Privacy Essentials

Control Access:

- Set who can see posts and profile
- Use "close friends" or "custom lists"
- Manage visibility and login alerts

What NOT to Overshare:

- Real-time location or vacation schedules
- Financial information and purchases
- Personal drama and relationships
- Work-related confidential information



Your Privacy Protection Roadmap

Immediate Actions (This Week):

- Change passwords on critical accounts
- Enable 2FA on important accounts
- Review social media privacy settings
- Install a password manager

Short-Term (This Month):

- Update all devices and apps
- Place credit freeze (Equifax, Experian, TransUnion)
- Audit app permissions and account settings

Trust But Verify – Every interaction, every link, every request.

