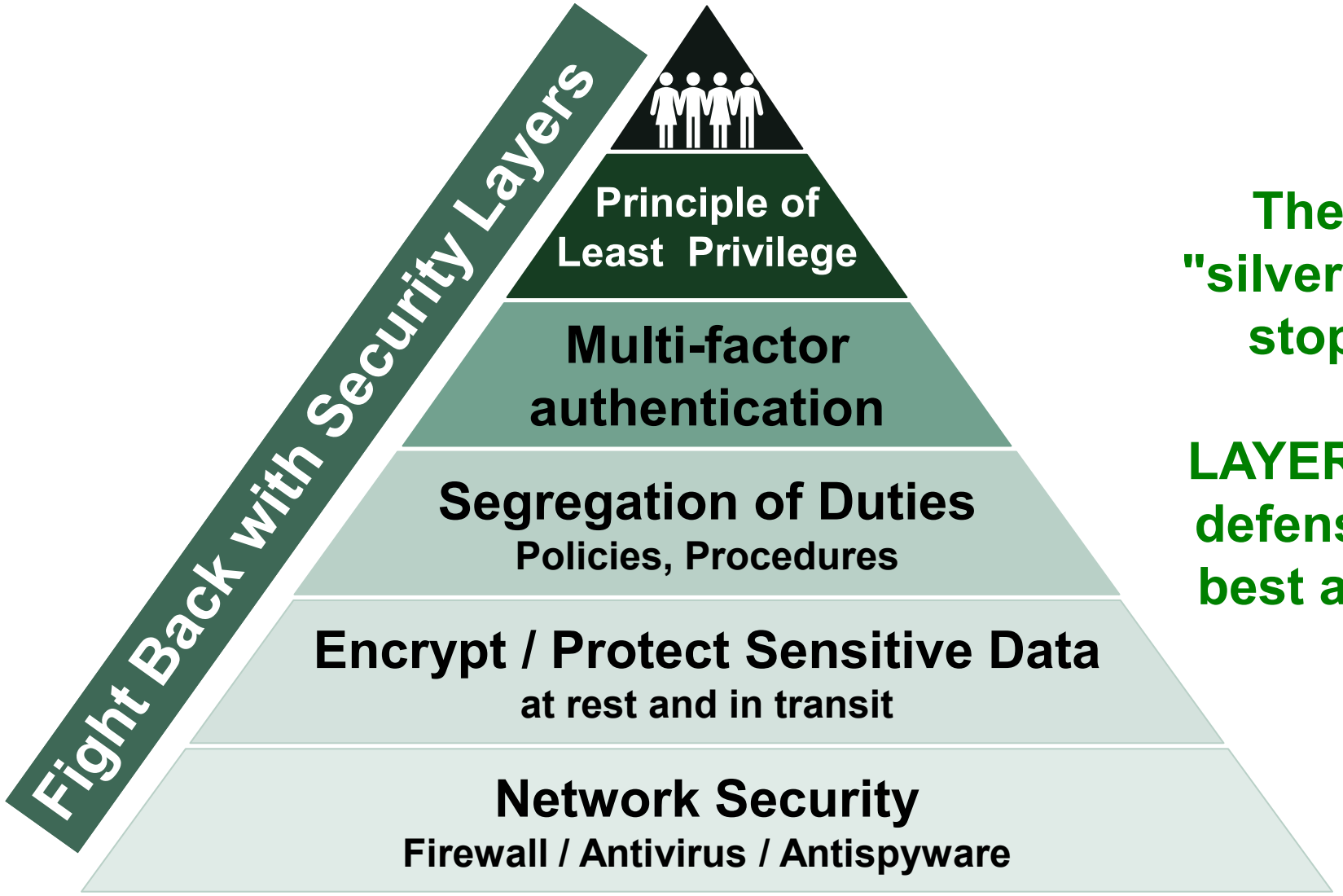
Appendix

Resources at your Fingertips

Resource	Link[1]
American Bankers Association (ABA)	https://www.banksneveraskthat.com/
Association for Financial Professionals (AFP) • 2021 Payments Fraud & Control Survey	https://www.afponline.org/publications-data-tools/reports/survey-research-economic-data/Details/payments-fraud/
Cybersecurity and Infrastructure Security Agency • CISA Insights	https://www.cisa.gov/insights
FBI: Coronavirus Updates	https://www.fbi.gov/coronavirus
Small Business Administration (SBA) • Fraud Alerts • Office of Inspector General Hotline	https://www.sba.gov/document/report-sba-programs-scams-fraud-alerts https://www.sba.gov/about-sba/oversight-advocacy/office-inspector-general/office-inspector-general-hotline
Treasury Perspectives Survey (2020) Strategic Treasurer and TD Bank	https://strategictreasurer.com/2020-treasury-perspectives/

[1] TD Bank does not control the content or privacy policies associated with any third-party websites provided.



There's no "silver bullet" to stop fraud.

LAYERING your defenses is the best approach.

TRUST | ADVICE | SECURITY

10 Common Risk Management Practices

- **Cultivate a Risk Management Culture** within the organization
- **Mandate Process Controls** including dual control and segregation of duties
- **Validate the security of a website's URL** and avoid public WiFi for banking and payments
- **Pick up the Phone** to authenticate **ALL** payment requests (internal & vendor)
- **Inspect Bank Accounts Daily** and reconcile frequently to spot potential fraud
- **Structure Bank Accounts** to isolate activities and leverage inherent controls
- **Use Fraud Deterrent Banking Services** like Positive Pay, ACH Blocks/Filters, etc.
- **Monitor Information** with credit reporting agencies and state record databases
- **Initiate Background Checks** on **ALL** employees and contractors
- **Notify the Bank & Law Enforcement** if you are under attack

TRUST | ADVICE | SECURITY

Mitigation Tips for Prominent Fraud Types

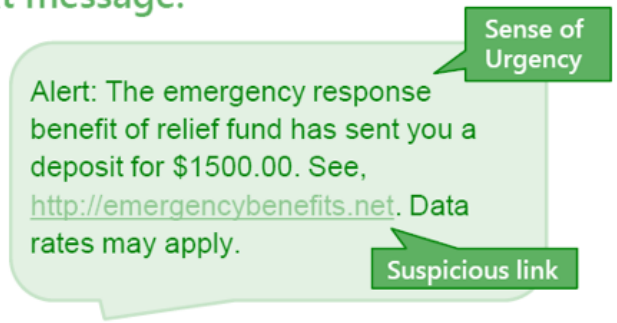
- Payee Positive Pay for Checks
- Positive Pay for ACH
- ePayables
- Reconciliation Services

- Multi-factor Authentication
- Segregation of duties via system user entitlements
- Timely and robust reporting

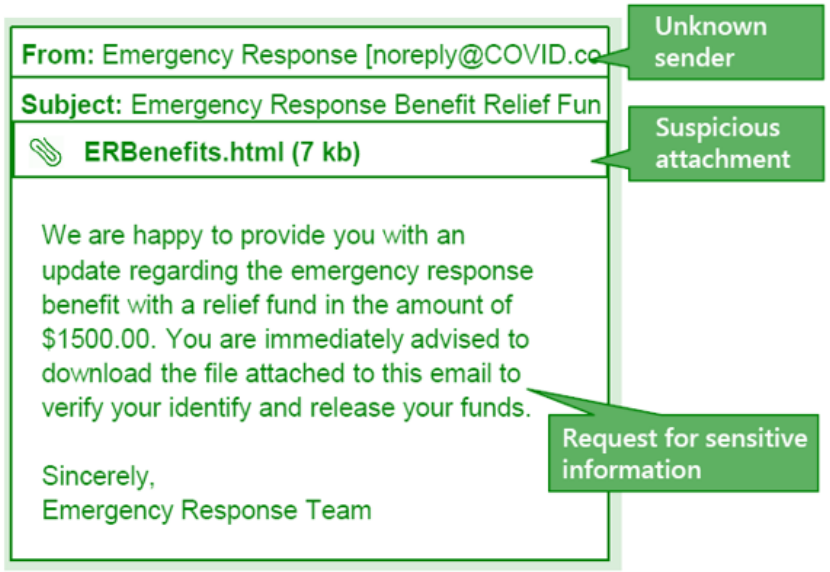
- Secure, central location for vendor payment instructions
- Encrypted data in transit and at rest

Cyber Threats: Phishing

Text message:



Email message :



Warning Signs for Suspicious Messages:

- ☑ Unknown senders
- ☑ Generic greetings
- ☑ Hidden email senders or suspicious links
- ☑ Attachments with suspicious extensions
- ☑ Requests for sensitive information
- ☑ Urgency or call to action
- ☑ Errors, or something being "off"

TRUST | ADVICE | SECURITY

Stages of BEC

Stage 1 – Compromising Victim Information and Email Accounts

Criminals access a victim's email account through social engineering or computer intrusion techniques. Criminals subsequently exploit the victim's email account to obtain information on the victim's financial institutions, account details, contacts and related information (or other info such as w2s).

Stage 2 – Transmitting Fraudulent Transaction Instructions

Criminals then use the victim's stolen information to email fraudulent wire transfer instructions to the financial institution in a manner appearing to be from the victim. To this end, criminals will use either the victim's actual email account they now control or create a fake email account resembling the victim's email.

Stage 3 – Executing Unauthorized Transactions

Criminals trick the victim's employee or financial institution into conducting wire transfers that appear legitimate but are, in fact, unauthorized. The fraudulent transaction instructions direct the wire transfers to the criminals' domestic or foreign bank accounts.

Source: VIPRE

Ransomware Mitigations – Defend Today, Secure Tomorrow

Actions for Today – Make Sure You're Not Tomorrow's Headline:

1. Backup your data, system images, and configurations and keep the backups offline
2. Update and patch systems
3. Make sure your security solutions are up to date
4. Review and exercise your incident response plan
5. Pay attention to ransomware events and apply lessons learned

Actions to Recover If Impacted – Don't Let a Bad Day Get Worse:

1. Ask for help! Contact CISA, the FBI, or the Secret Service
2. Work with an experienced advisor to help recover from a cyber attack
3. Isolate the infected systems and phase your return to operations
4. Review the connections of any business relationships (customers, partners, vendors) that touch your network
5. Apply business impact assessment findings to prioritize recovery

Actions to Secure Your Environment Going Forward – Don't Let Yourself be an Easy Mark:

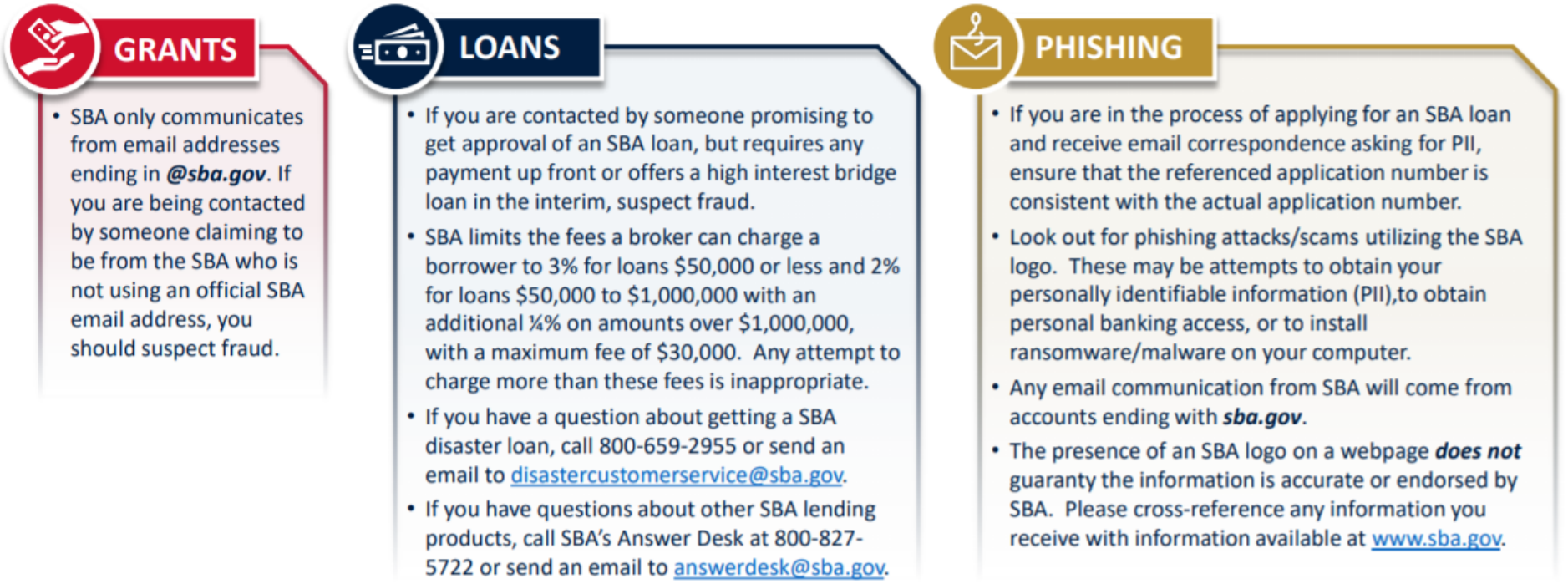
1. Practice good cyber hygiene; backup, update, whitelist apps, limit privilege, and use multifactor authentication
2. Segment your networks; make it hard for the bad guy to move around and infect multiple systems
3. Develop containment strategies; if bad guys get in, make it hard for them to get stuff out
4. Know your system's baseline for recovery
5. Review disaster recovery procedures and validate goals with executives

Source: www.CISA.gov

SBA: Be Aware of Scams and Fraud Schemes

The Office of Inspector General recognizes that we are facing unprecedented times and is alerting the public about potential fraud schemes related to economic stimulus programs offered by the U.S. Small Business Administration in response to the Novel Coronavirus Pandemic (COVID-19). The Coronavirus Aid, Relief, and Economic Security Act (CARES Act), the largest financial assistance bill to date, includes provisions to help small businesses. Fraudsters have already begun targeting small business owners during these economically difficult times.

Be on the lookout for grant fraud, loan fraud, and phishing.



Source: www.SBA.gov

TRUST | ADVICE | SECURITY

Tips to prevent payment fraud and cybercrimes.

Payment fraud and cybercrime are always on the rise and criminal methods are always changing.

That's why it's essential to keep up with best practices to combat them. Know what you're up against and assess your readiness using these tips. Together, we can combat illegal activity and keep accounts secure.

Prevention begins with people

- Educate and train employees at regular intervals—this is key to reducing human error
- Treat security awareness as an ongoing program, not a single project
- Create and sustain a culture that enables employees to build awareness and apply best practices
- Foster a culture that supports and rewards a "human firewall" that is proactive and pre-emptive against fraud and cybercrime
- Empower employees to report suspicious activities and enforce policies to reduce fraud risk

Electronic Payment Fraud

(includes wires and ACH)

- Activate ACH Positive Pay on all accounts, including debit blocks and filters
- Employ dual controls
- Sign up for automated alerts, same-day reporting
- Use a separate account for ACH activity only, especially payroll
- Establish templates for pre-authenticated payment instructions
- Centralize transactions in Accounts Payable to maintain a clean audit trail
- Explore UPIC technology for ACH credits

Tips to prevent payment fraud and cybercrimes.

Check Fraud

- Use Check Positive Pay, ideally with payee verification
- Set default for exceptions to "do not pay"
- Automate check processing or outsource to reliable service providers
- Use security features on checks and secure when not in use
- Activate ACH Positive Pay for checking accounts to avoid unauthorized electronic transfers

Card Fraud

- Use Address Verification Services (AVS)
- Request CVV/CVC for Card Not Present (CNP) Transactions
- Send confirmations independent of transactions
- Process refunds only to the original card number
- PCI Compliance is required of all merchants

General Fraud

(regardless of payment type or fraud attack vector)

- Establish policies and procedures to identify, report, and remediate fraud and cybercrime incidents
- Use dual- or multi-factor authentication
- Segregate duties and limit access to systems or sensitive information according to job roles
- Verify payment instructions verbally with suppliers using known contact information
- Be alert to social engineering attacks such as Business Email Compromise (BEC)
- Reconcile accounts frequently, if not daily

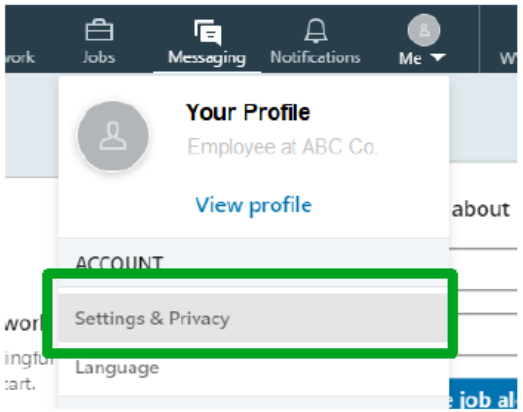
TD Bank

America's Most Convenient Bank®

Social Media Smart-Card
LinkedIn

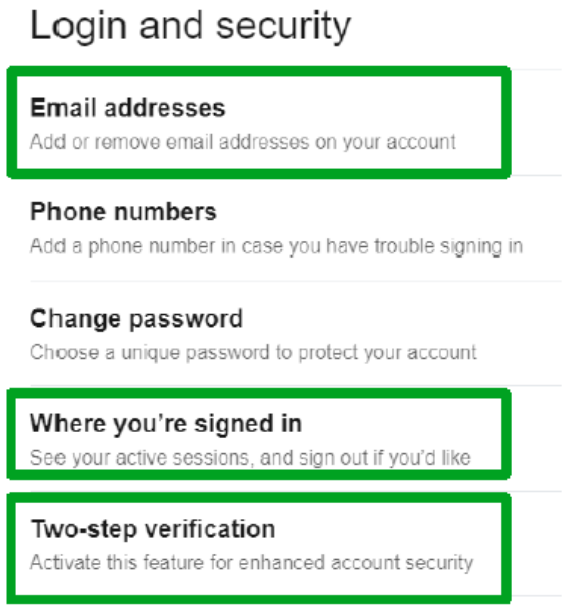
Limit what you share.

The following best practices will help you protect yourself on LinkedIn and reduce the risk of your personal information being exposed online.



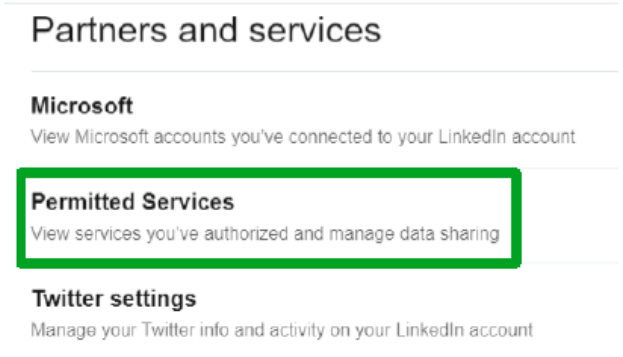
Access Settings & Privacy

Select your profile icon located toward the top right then select Settings and Privacy from the drop-down menu



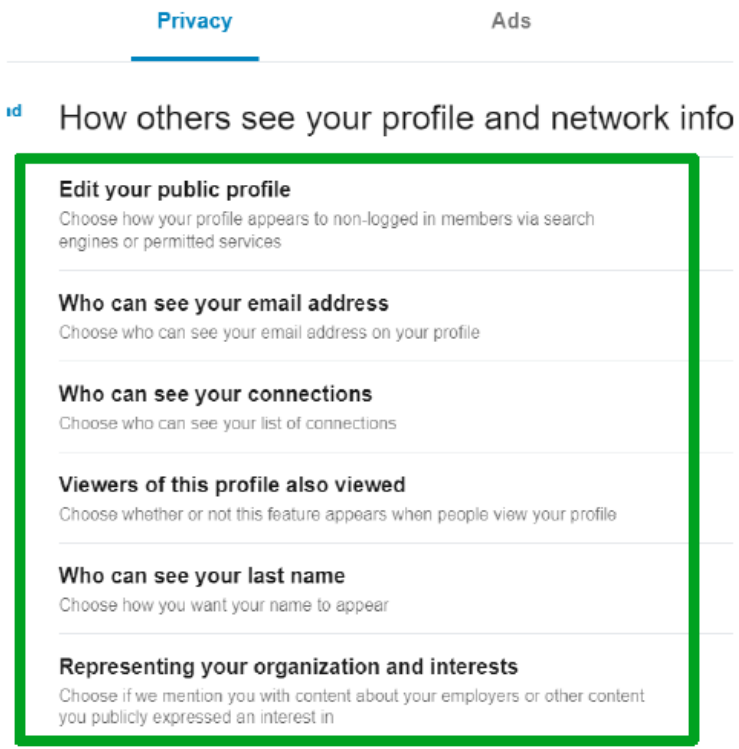
Login and Security

- Use a personal email address to register and maintain your LinkedIn account
- Review where you're signed in for account activity and remove any suspicious logins
- Enable Two-step verification; a code will be sent to your phone when you log into LinkedIn



Partners and Services

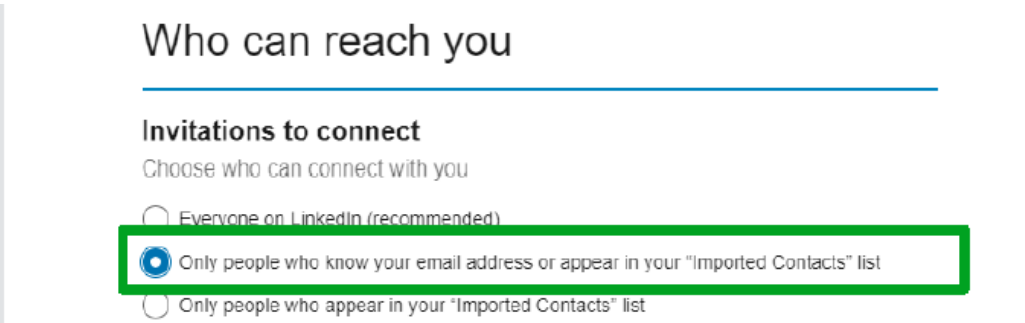
- Review Permitted Services and remove any third-party applications you do not recognize or want sharing data regarding your LinkedIn activity



Privacy Settings

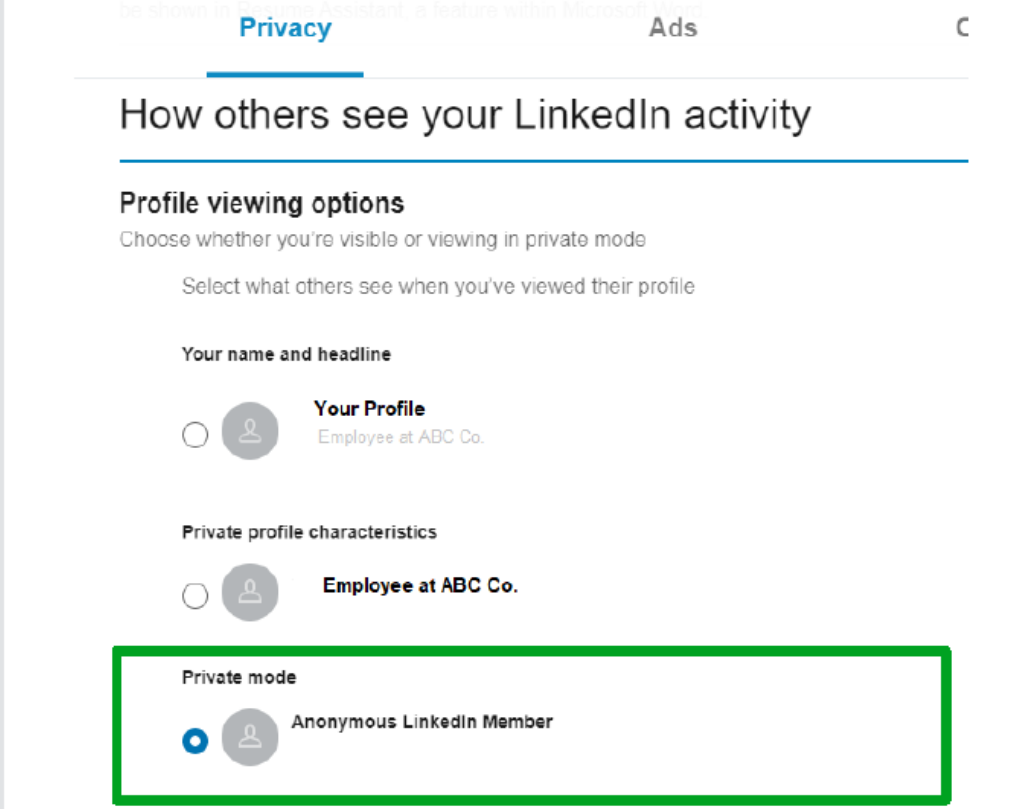
- ☑ Limit who can see your email address under Who can see your email setting
- ☑ Change Who can see your connections setting to Only you
- ☑ Select No for Viewers of this profile also viewed setting
- ☑ Limit your activity exposure by selecting No for Representing your organization and interests setting
- ☑ Select No for Profile visibility off LinkedIn setting

Minimize the amount of personal information posted, limiting job descriptions, previous work, and education beyond what is necessary



Communication Settings

- [x] Select Only people who know your email address or appear in your imported contacts list option



Profile Viewing Options

- [x] Disable Your profile public visibility
- [x] Limit the data visible to non-connections by selecting Your Connections only for Manage active status setting

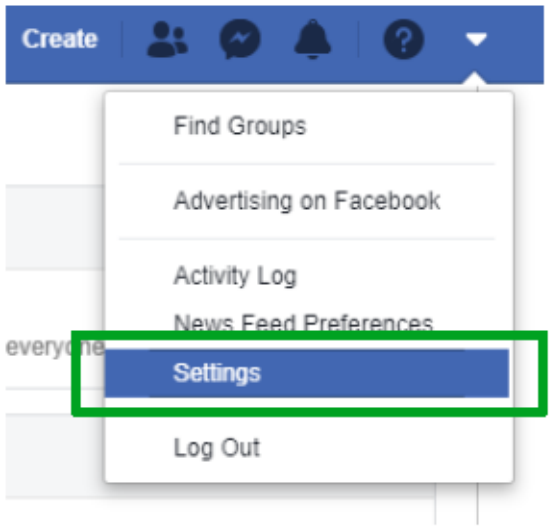
Users can still contact you via LinkedIn's private messaging platform with the above-mentioned settings enabled

Social Media Smart-Card

Facebook

Limit what you share.

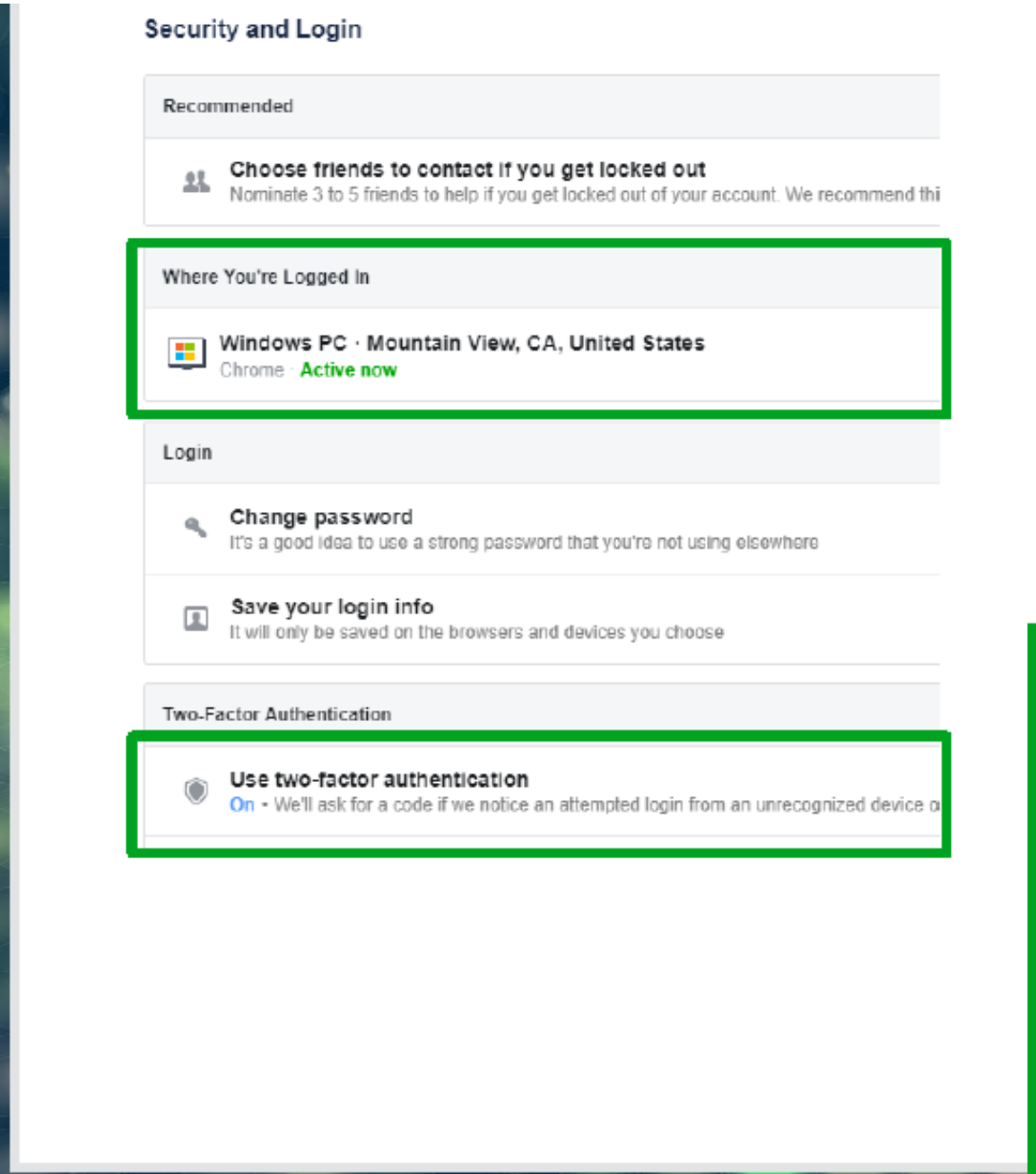
The following best practices will help you protect yourself on Facebook and reduce the risk of your personal information being exposed online.



Access Settings

Click the dropdown arrow located toward the top far right blue menu then click Settings

Settings include: General, Security and Login, Your Facebook Information, Privacy



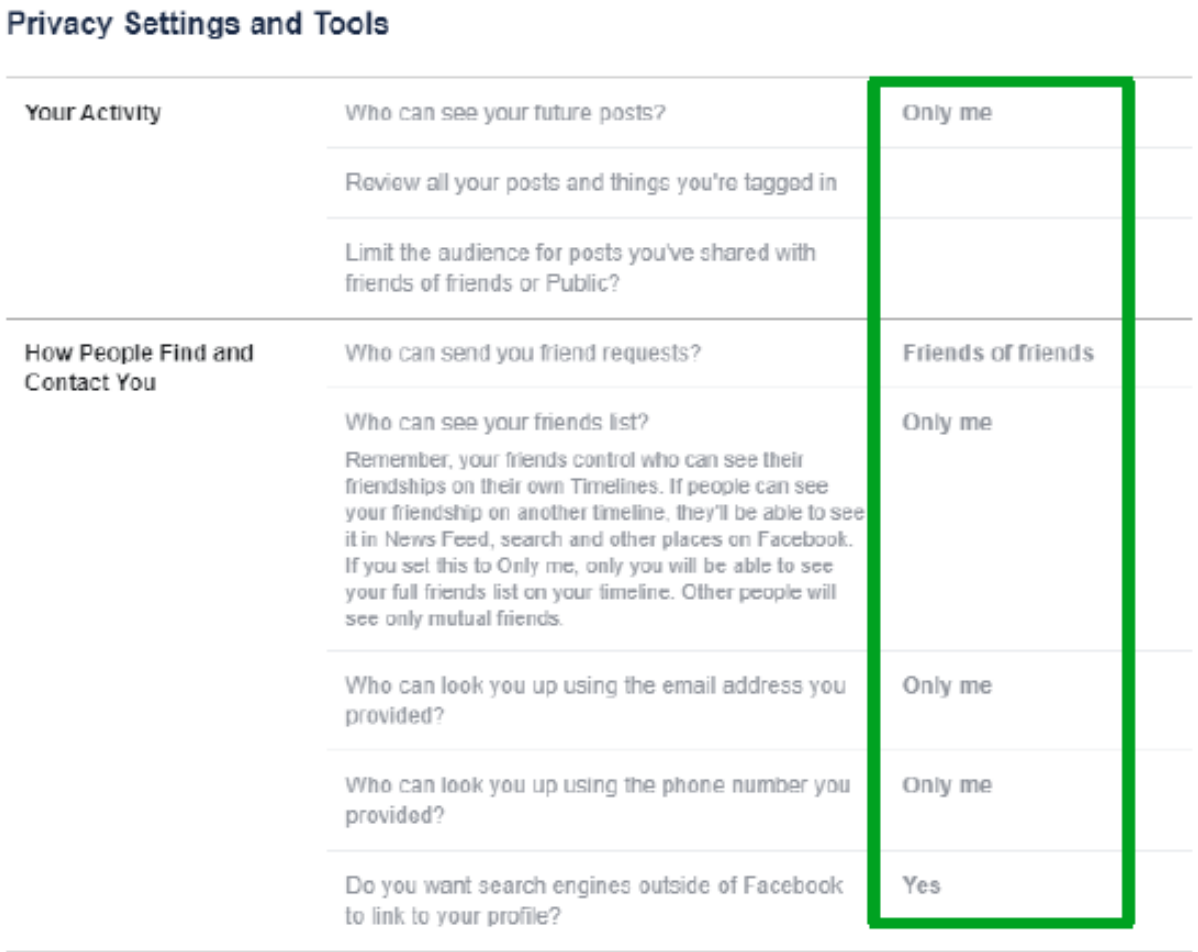
Security and Login

- Confirm where you are logged in and disable any sessions you do not recognize
- Enable two-factor authentication; a code will be sent to your phone when you log into Facebook

Did you know?

A common method of an attack is via Facebook Messenger, with malware links in messages with titles like: "is this video you".

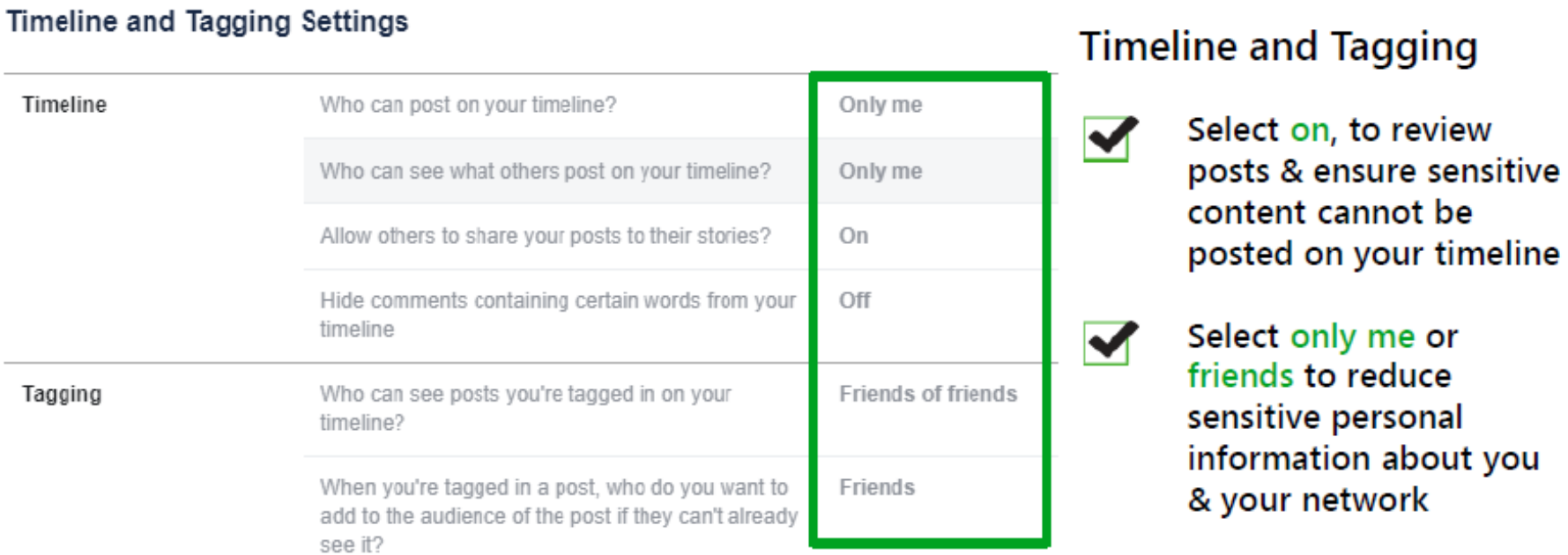
Always use caution when clicking on links in both Messenger and in posts on yours or other's walls. When in doubt, delete.



Privacy

- ☑ Select only me or friends to reduce unwanted invitations and limit who can send you requests

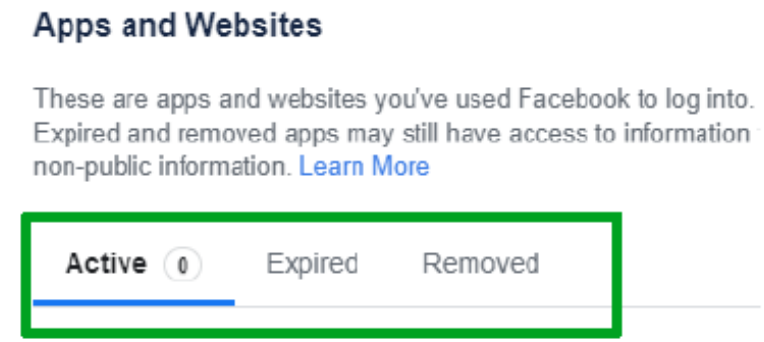
Fraudsters can look you up by using a known email or phone number to find your personal account



Timeline and Tagging

- Select on, to review posts & ensure sensitive content cannot be posted on your timeline
- Select only me or friends to reduce sensitive personal information about you & your network

Fraudsters will try and identify pictures of you & establish patterns of behavior between you and your connections



App and Websites

- Modify the amount of information provided or remove the app entirely if you no longer use it

Third-party apps are often compromised in attacks and used to deliver malware to phones and computers - Avoid participating in informal surveys or quizzes that ask for historical data