



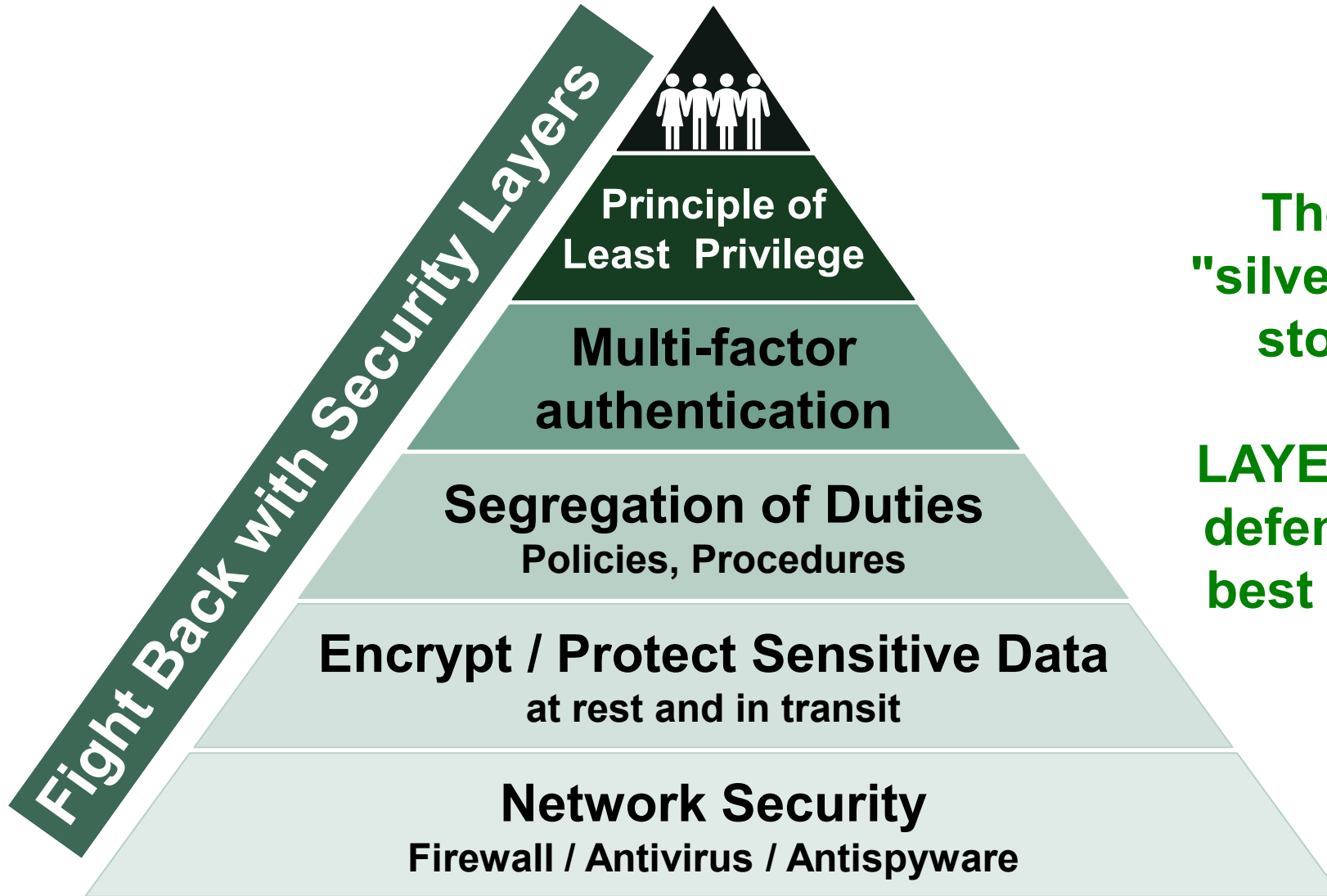
Appendix



Resources at your Fingertips

Resource	Link ¹
American Bankers Association (ABA)	https://www.banksneveraskthat.com/
Association for Financial Professionals (AFP) <ul style="list-style-type: none"> 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 <ul style="list-style-type: none"> CISA Insights 	https://www.cisa.gov/insights
FBI: Coronavirus Updates	https://www.fbi.gov/coronavirus
Small Business Administration (SBA) <ul style="list-style-type: none"> 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:

Alert: The emergency response benefit of relief fund has sent you a deposit for \$1500.00. See, <http://emergencybenefits.net>. Data rates may apply.

Sense of Urgency

Suspicious link

Email message :

From: Emergency Response [noreply@COVID.co
Subject: Emergency Response Benefit Relief Fun

ERBenefits.html (7 kb)

We are happy to provide you with an update regarding the emergency response benefit with a relief fund in the amount of \$1500.00. You are immediately advised to download the file attached to this email to verify your identify and release your funds.

Sincerely,
Emergency Response Team

Unknown sender

Suspicious attachment

Request for sensitive information

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

TRUST | ADVICE | SECURITY



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

TRUST | ADVICE | SECURITY



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.



GRANTS

- SBA only communicates from email addresses ending in @sba.gov. If you are being contacted by someone claiming to be from the SBA who is not using an official SBA email address, you should suspect fraud.



LOANS

- If you are contacted by someone promising to get approval of an SBA loan, but requires any payment up front or offers a high interest bridge loan in the interim, suspect fraud.
- SBA limits the fees a broker can charge a borrower to 3% for loans \$50,000 or less and 2% for loans \$50,000 to \$1,000,000 with an additional ¼% on amounts over \$1,000,000, with a maximum fee of \$30,000. Any attempt to charge more than these fees is inappropriate.
- If you have a question about getting a SBA disaster loan, call 800-659-2955 or send an email to disastercustomerservice@sba.gov.
- If you have questions about other SBA lending products, call SBA's Answer Desk at 800-827-5722 or send an email to answerdesk@sba.gov.



PHISHING

- If you are in the process of applying for an SBA loan and receive email correspondence asking for PII, ensure that the referenced application number is consistent with the actual application number.
- Look out for phishing attacks/scams utilizing the SBA logo. These may be attempts to obtain your personally identifiable information (PII), to obtain personal banking access, or to install ransomware/malware on your computer.
- Any email communication from SBA will come from accounts ending with sba.gov.
- The presence of an SBA logo on a webpage **does not** guaranty the information is accurate or endorsed by SBA. Please cross-reference any information you receive with information available at www.sba.gov.

TRUST | ADVICE | SECURITY

Source: www.SBA.gov

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



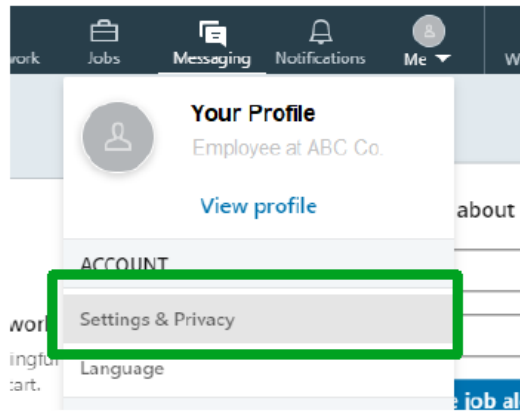
America's Most Convenient Bank®



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

Email addresses

Add or remove email addresses on your account

Phone numbers

Add a phone number in case you have trouble signing in

Change password

Choose a unique password to protect your account

Where you're signed in

See your active sessions, and sign out if you'd like

Two-step verification

Activate this feature for enhanced account security

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

Microsoft

View Microsoft accounts you've connected to your LinkedIn account

Permitted Services

View services you've authorized and manage data sharing

Twitter settings

Manage your Twitter info and activity on your LinkedIn account

Partners and Services



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

id How others see your profile and network info

Edit your public profile
Choose how your profile appears to non-logged in members via search engines or permitted services

Who can see your email address
Choose who can see your email address on your profile

Who can see your connections
Choose who can see your list of connections

Viewers of this profile also viewed
Choose whether or not this feature appears when people view your profile

Who can see your last name
Choose how you want your name to appear

Representing your organization and interests
Choose if we mention you with content about your employers or other content you publicly expressed an interest in

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

Who can reach you

Invitations to connect

Choose who can connect with you

- Everyone on LinkedIn (recommended)
- Only people who know your email address or appear in your "Imported Contacts" list
- Only people who appear in your "Imported Contacts" list

Communication Settings

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

be shown in Resume Assistant, a feature within Microsoft Word

Privacy

Ads


How others see your LinkedIn activity

Profile viewing options

Choose whether you're visible or viewing in private mode

Select what others see when you've viewed their profile


Your name and headline

-  **Your Profile**
Employee at ABC Co.

Private profile characteristics

-  **Employee at ABC Co.**

Private mode

-  **Anonymous LinkedIn Member**

Profile Viewing Options

- Disable** Your profile public visibility
- 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



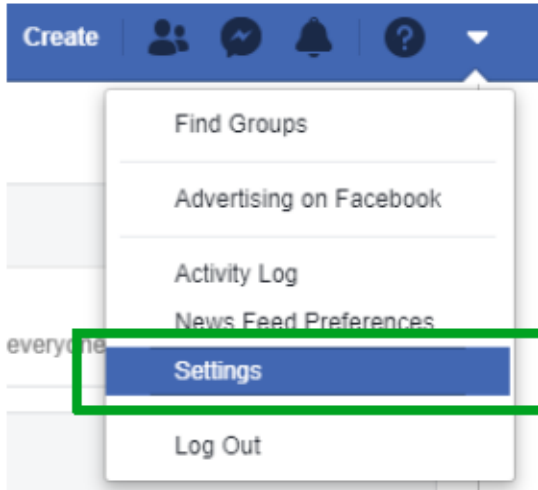
Social Media Smart-Card

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

Recommended

Choose friends to contact if you get locked out
Nominate 3 to 5 friends to help if you get locked out of your account. We recommend thi

Where You're Logged In

Windows PC · Mountain View, CA, United States
Chrome · **Active now**

Login

Change password
It's a good idea to use a strong password that you're not using elsewhere

Save your login info
It will only be saved on the browsers and devices you choose

Two-Factor Authentication

Use two-factor authentication
On · We'll ask for a code if we notice an attempted login from an unrecognized device or

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 Settings and Tools

Your Activity	Who can see your future posts?	Only me
	Review all your posts and things you're tagged in	
	Limit the audience for posts you've shared with friends of friends or Public?	
How People Find and Contact You	Who can send you friend requests?	Friends of friends
	Who can see your friends list? Remember, your friends control who can see their friendships on their own Timelines. If people can see your friendship on another timeline, they'll be able to see it in News Feed, search and other places on Facebook. If you set this to Only me, only you will be able to see your full friends list on your timeline. Other people will see only mutual friends.	Only me
	Who can look you up using the email address you provided?	Only me
	Who can look you up using the phone number you provided?	Only me
	Do you want search engines outside of Facebook to link to your profile?	Yes

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 Settings

Timeline	Who can post on your timeline?	Only me
	Who can see what others post on your timeline?	Only me
	Allow others to share your posts to their stories?	On
	Hide comments containing certain words from your timeline	Off
Tagging	Who can see posts you're tagged in on your timeline?	Friends of friends
	When you're tagged in a post, who do you want to add to the audience of the post if they can't already see it?	Friends

Timeline and Tagging



Select **on**, to review posts & ensure sensitive content cannot be posted on your timeline

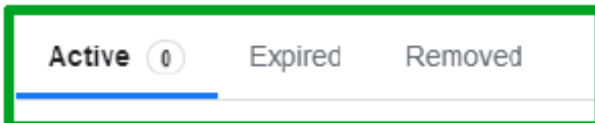


Select **only me** or **friends** to reduce sensitive personal information about you & your network

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

Apps and Websites

These are apps and websites you've used Facebook to log into. Expired and removed apps may still have access to information non-public information. [Learn More](#)



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**