Security Bank of California
Internet Banking
Security Awareness
INTRODUCTION

- Fraudsters are using increasingly sophisticated and malicious techniques to thwart existing authentication controls and gain control of client accounts to transfer money.

- Many schemes target small to medium-sized business clients since their account balances are generally higher than consumer accounts, and transaction activity is greater, making it easier to hide fraudulent transfers.

- Security Bank of California is committed to helping you be aware of these risks and liabilities, some risk mitigation techniques, and response strategies should online fraud be encountered.
Some Online Risks

A. “Malware” – Malicious Software
   1. Viruses
   2. Keystroke loggers – Zeus Trojan

B. Phishing (SpearPhishing, SMiShing, Vishing, etc.)

C. Browser Attacks
   1. “Drive-by” download
   2. “Man-in-the-middle”

D. All computers are susceptible. Microsoft Windows-based machines are primary targets, due to their prevalence, but attacks on Apple, Android, and other operating systems are increasing as they become increasingly popular user options.
Liabilities

- You are responsible for your computer(s) and Internet access facilities.

- Business client liabilities are established by contract, Security Bank of California’s Commercial Cash Management Enrollment Form and Agreement. Consumer regulatory protections, such as Regulation E, do not apply to businesses, not even to sole-proprietors/practitioners.
Security Options

A. End-user Precautions (YOU)
   1. Use a Secure Computer
      a. Keep Operating System (OS) and browser software current
      b. Watch for and Update “Patches” for security (application software as well as OS and browser)
      c. Maintain anti-malware suite w/current “pattern files” (Trend Micro, Symantec/Norton, McAfee, Kaspersky)
      d. Preferably isolated to online banking ONLY – NO SURFING!
      e. Never use a public computer (hotel, café) for business banking
      f. Be very careful when using unknown wireless networks, even with your own mobile device. Be sure to use SSL connections (httpS) and maintain anti-malware and firewall on your device. Consider Virtual Private Network (VPN) for secure communications when possible
      g. Use a firewall (OS-supplied at a minimum; router preferred)
Security Options (Cont.)

2. If you have more than one online banking account, use a separate login name and password for each so the breach of one does not compromise all. Consider a complex/obscure Login ID to make guessing more difficult.

3. Use strong passwords
   a. At least eight characters, no more than 15, including:
      i. At least one upper and one and lower-case letter
      ii. At least one number
      iii. Required to change every 90 days
   b. No words from dictionary
   c. No personal information, like license plate number, birthdate, anniversary, children’s names, etc. Much of this can be found on Social Media sites.
   d. It may help to think of a sentence that will be easy to remember, and use the first letter of each word, including some punctuation (acronym). For example: “It’s a really nice day June 27!” could become “IarndJ27!”, and that could be a fairly secure password.
4. Set realistic ACH transaction limits, number/amount, daily/monthly
5. Restrict user access to their necessary functions, and require individual Login Name and Password (no sharing of credentials).
6. Never click on a link in any warning e-mail purportedly from any bank (or any other source – “ACH”, “Fed”, “IRS”). Call instead to ensure it is legitimate.
7. If your computer is acting sluggish and/or you’re getting lots of unexplained pop-up messages, do not use for online banking until you get it checked out by a computer security specialist. These may be signs of malware running on your computer.
8. Never respond to e-mails requesting personal information. No reputable business will ask for confidential information this way.
9. Security Bank of California will never initiate contact with you via e-mail, telephone, or otherwise to ask for any confidential information.
Security Options (Cont.)

B. Security Bank of California incorporates a robust set of features to support and facilitate security.

1. Secure Access – Look for [https://](https://) and Padlock
2. Anti-Phishing Phrase
3. Login ID/Password (Complex/strong recommended)
4. Computer Registration (per use or future use option)
5. Security Alerts such as:
   - Login name change, password change, invalid password, profile update, new user, and more.
6. Limit number and amount of transactions, per day and per month
7. Dual Authorization
8. Risk and Fraud Analytics – “Behavioral Modeling” Software
Risk Mitigation

Some other thoughts to reduce your risks:

- Check accounts frequently – at least daily
- Determine Company risk tolerance/aversion vs. convenience and implement recommendations and Security Bank of California security features accordingly
- Educate others with access to company computing resources regarding risks and your policies/procedures
- Establish response plan if security/fraud event is detected
- Consider insurance to cover any losses – contact your insurance agent
Contacts

In the event of suspected online banking security issues or fraud, reach out ASAP to:

- (888) 459-BANK (2265) or (877) 461-SBOC (7262)
- E-mail online@securitybankca.com
Summary

Risks Are Evolving
- Basic techniques have been around quite a while, but sophistication is increasing and targeting is becoming much more focused
- New attacks as yet unknown

Defenses Must Also Evolve
- There is no “magic bullet”. Security must be ongoing, and defense in layers
- There must be ongoing development of security features and options

Awareness Is Vital
- Understand risks and liabilities, and options to mitigate
- Educate all your authorized users

Take Action
- Increased implementation of security features by end-users is essential
  - Work with your IT staff or outside specialists, as needed, to assess and remediate risks in your environment
  - Work with Security Bank of California to implement security features to suit your risk tolerance
- Plan an event response so you may react quickly to any threats or attacks
A Few Resources

  Fraud Advisory for Businesses – Corporate Account Takeover

- [http://www.fcc.gov/cyberforsmallbiz](http://www.fcc.gov/cyberforsmallbiz)
- [http://www.antiphishing.org](http://www.antiphishing.org)
- [http://www.onguardonline.gov/topics/overview.aspx](http://www.onguardonline.gov/topics/overview.aspx)
Disclaimer

This presentation is for training purposes only, and is intended solely for the information of our online banking clients. These materials have no effect on existing contracts or Bank policies and neither amend nor modify them, nor do they serve, and should not be construed, as legal advice.