SECURITY
NATIONAL BANK

Visit SNBconnect.com/Webinars

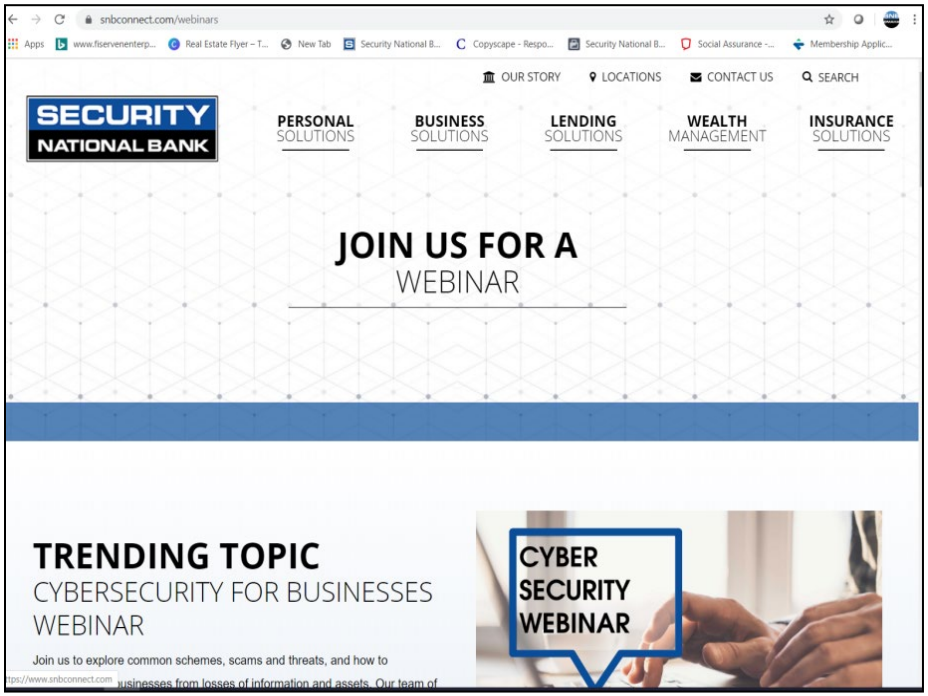
402-344-7300 844-SNB-1964

Today's Webinar

Today's Webinar will be recorded and posted to our website.

Please use the Zoom features to ask questions at any time during the presentation.

We'll address them during or at the end of our presentation.



SNBconnect.com/webinars

SECURITY NATIONAL BANK

Timeliness: Why Now

- Today's pandemic environment means more people are working remotely, which may present a number of security issues for businesses:
  - Employees may be using personal devices and computers.
  - Less supervision, inhibition.
  - Blurred lines between professional and personal use and communications.
  - Increased reliance on electronic means to operate.

SECURITY NATIONAL BANK

Agenda

- **Security:** How access is gained to systems.
- **Fraud:** What happens when access is gained, enabling criminals to potentially steal information and/or money.

SECURITY NATIONAL BANK

Our Team

- **Amy Stephenson**
  AVP, Senior Information Security Analyst
- **Fran Branan**
  VP, Director of Operations & Information Security
- **Megan Froehlich**
  VP, Sales Director and Cash Management
- **Mike Mann**
  VP, Cash Management Operations Manager
- **Jarrod Daake, Five Nines**
  Director of Operations – Greater Nebraska

SECURITY NATIONAL BANK

Security Risks

- Passwords
- Phishing and Spear Phishing
- Network Security
- Malware
- Ransomware

SECURITY
NATIONAL BANK

Best Practices: Security-Passwords

- Educate employees on the use of passwords.
- Prohibit sharing usernames and passwords for online banking and other important systems.
- Establish procedures to control employee access to secure logins and sites if employment status changes.

Train Employees:

- Use a phrase that can be remembered easily and protect the account, like this: **$unWalkRainDriv3**
- Use a different password for each website and change passwords several times a year.
- Never share username and passwords for online services with third-party providers.

SECURITY NATIONAL BANK

Security: Phishing and Spear Phishing

- **Phishing:** Fraudulent practice of sending emails pretending to be from a reputable company to induce individuals to reveal information.

- **Spear Phishing:** Fraudsters send emails that are tailored to the receiver and appear to be from a known source or trusted sender to induce a targeted individuals to reveal confidential information. Phishing is the third most common cause of data breaches.

SECURITY
NATIONAL BANK

Security: Phishing and Spear Phishing

- Employee Training and Testing
  - Conduct regular information security training and phishing tests on all employees.
  - Train all new employees at time of hire.
  - Provide additional training to employees or departments that repeatedly click in phishing emails.

- SPAM filtering and other security measures
  - Check with your email vendor to see what security measures they provide.
    - Spam filtering, anti-virus, data loss protection, email encryption.

SECURITY NATIONAL BANK

Security: Network Security

- Install a dedicated, actively managed firewall if using a broadband or dedicated connection to the internet such as DSL or cable. A firewall limits the potential for unauthorized access to a network and computers.

- Limit administrative rights on users' workstations to help prevent unauthorized or inadvertent downloading of malware or other viruses.

SECURITY
NATIONAL BANK

Security: Network Security

- Install commercial anti-virus, spyware detection and desktop firewall software on all computer systems. Free software may not provide the most current threat protection.

- Ensure security suite software pages and computer programs are patched regularly.

- Consider utilizing a third-party network monitoring company to detect and alert you to unusual or suspicious network activity

SECURITY
NATIONAL BANK

Security: Malware

- **Malware:** Any software intentionally designed to case damage to a computer server, client or network. Common types include:
  - Computer virus
  - Worms
  - Trojan horses
  - Spyware
  - Scareware

SECURITY NATIONAL BANK

Security: Ransomware

- **Ransomware:** A type of Malware that threatens to block access or publish the victim's data unless a ransom is paid.
  - Every 14 seconds a business is targeted with ransomware.
  - Half of ransomware attacks affect over 20 company devices.
  - It's a myth that once a ransom is paid, the victim will no longer be targeted.

SECURITY NATIONAL BANK

Fraud

- Email Compromise
- Debit and Credit Cards
- Checks
- Wire and ACH
- Incident Response Planning
- General Best Practices

SECURITY NATIONAL BANK

Fraud: Email Compromise

- Phishing emails gain access to a business email account and steal information, account access, funds.
- Email compromise is the most frequent method of attack because scammers have the technology and mechanisms today to be more convincing.
- Real-time payment networks mean that money can move quickly.
- Even after you've recovered the account, the attacker may have added back-door entries to resume control of the account.

SECURITY NATIONAL BANK

Fraud: Email Compromise

Case Study#1:

An executive or finance department employee receives an email from a vendor or another employee saying that they should make a significant transfer of funds to an external account.

The email often contains an urgent message.

SECURITY NATIONAL BANK

Fraud: Email Compromise

Case Study #2:

An employee receives an email asking them to click on the link to receive a free lunch.

The employee tells you that they clicked on the link and it didn't go anywhere.

SECURITY NATIONAL BANK

Fraud: Debit and Credit Cards

- Increased reliance on online and mobile shopping, fraudsters have moved to target "card-not-present" payments.
- Customer experience and convenience often is prioritized over security.
- Liability has shifted to 60% for merchants, up from 40% in 2015, so the retail community is more aware.
- Cyber criminals steal information harvested from online merchants, including stored payment data. Criminals sell the card numbers on the dark web.

SECURITY NATIONAL BANK

Fraud: Debit and Credit Cards

Case Study #3:

You are purchasing additional hand sanitizer online since it is hard to find it in stores. You checked with all your normal online suppliers but they are all out. You Google it and find a supplier that has what you need. You make the purchase using your corporate credit card.

Within a few minutes your start getting texts about possible fraud transactions on your card.

SECURITY NATIONAL BANK

Fraud: Checks

Case Study #4:

You pull up your account in the morning and see that it has a negative balance. You realize that you have check 8465 that doesn't match what you issued. The amount should have been $47.89 and it ran through as $54,987.00.

SECURITY NATIONAL BANK

Fraud: Wire

Case Study #5

Security National Bank receives a request to process a wire for XYZ company. We take the information and follow up with a call back to the phone number on record. We read back the information and it is verified. The wire is processed.

Several days later we receive a call from XYZ company stating its vendor never received the wire. SNB verifies the wire was sent with the instructions provided. XYZ finds out that there was an email compromise and the new wire instruction were not provided by the vendor.

SECURITY NATIONAL BANK

Fraud: Email Compromise - Regaining Control

1. Block the user account from signing in
2. Reset the User Password
   - Do not send the new password via email
   - Make sure it's a strong password
   - Do not reuse a password
   - Consider enabling Multi-Factor Authentication
3. Remove suspicious email forwarding addresses
4. Disable any suspicious inbox rules
5. Unblock the user from sending email
6. Verify Sent items.
7. Consider notifying your contact list to ensure they are on alert, too.

SECURITY NATIONAL BANK

Incident Response Planning

Have a plan in place for different scenarios, including:

1. Your company email has been hacked. You have a vendor report that you sent an email to change your bank account information when they pay their invoice. What is your plan?
2. There is ransomware on an employee's computer. What is your plan?
3. You receive word that you had a fraudulent ACH file transmitted. What is your plan?

Don't wait until it happens.

SECURITY NATIONAL BANK

Best Practices: Email

- Train employees to be suspicious.
- Verbally or otherwise verify financial requests.
- Exercise special caution to those emails purporting to be from a financial institution, government department or other government agency.
- Never reveal usernames, passwords, PIN codes, answers to challenge questions and similar information via email.
- Do not open unknown or unexpected file attachments or click on web links.

SECURITY NATIONAL BANK

Best Practices: Banking Tools

- Reconcile all transactions daily.
  - Business online banking
  - Business mobile banking

- Take further steps to help monitor your account
  - Account eAlerts

- ACH Filter
- Positive Pay

Visit SNBconnect.com/Online-Education-Center for tutorial videos on these tools

SECURITY NATIONAL BANK

Best Practices: ACH

- Dual control for ACH and wire transfers
  - Transaction originator and separate transaction authorizer.

- For those originating ACH or wires, or a large number of online transactions, use a standalone, dedicated and secured computer system.
  - Not connected to email, non-financial sites or limited company network access.

SECURITY NATIONAL BANK

Best Practices: ACH

- Do not process payment changes from clients, vendors or employees without directly verifying the change.
  - NACHA rules require a valid authorization to be on file before a company can originate transactions to business or consumer accounts.
  - Changes to an authorization should be requested in writing.
  - A new authorization should be obtained before implementing any change.
  - Considering requesting a blank check with the new authorization.

SECURITY NATIONAL BANK

Q&A

Look for our a survey emailed to you after the webinar. Your feedback is important to us.

SECURITY NATIONAL BANK

Visit SNBconnect.com/Webinars

402-344-7300 844-SNB-1964