

# Mitigate, Recognize and React to Identity Theft



*Lucie Hannigan, SVP Treasury Management  
Janet Butland, VP Market Manager*



*11/06/2017*



*What know-how can do®*

# Mitigate Fraud Risk

Have you assessed your risks and taken appropriate action to secure yourself, your business and organization?

- Private vs. Public Information
- Know your environment
- Practice Cleaning and Clear Outs



# Home Security Checklist

- Always update your computer software; the operating system, internet browser, Adobe Acrobat, Flash, Java, antivirus, etc.
- Create strong passwords for your online accounts and never share them with anyone.
- Use different passwords for online banking than you use for social media sites or email.
- Shred any documents that contain your personal information, instead of putting them in the garbage.
- Whether you are on a cell phone or talking to another individual, be aware of your surroundings when discussing your personal information in public.
- Check your credit report at least once per year at [Annualcreditreport.com](http://Annualcreditreport.com) - it's free!
- If you have a wireless network at home, be sure that you use strong encryption, change any default passwords, and update any default security settings as appropriate.



# Take Control

Ask questions and be aware of controls available through your bank, mobile applications and card programs.

- Lock misplaced cards
- Set transaction limits
- Block International transactions
- Use Alerts

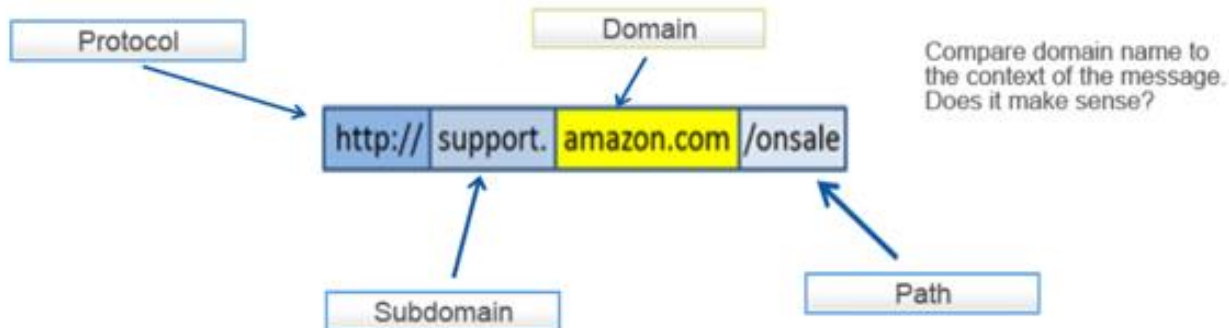


# How to detect malicious links

Phishing scams often succeed because end users don't know how to tell a valid link from a fake one. Phishers use fake links to fool people into clicking on what looks like a valid address that actually goes to a malicious website instead. **Identifying the Domain is the most effective method to detect phishing emails.**

## What do you need to know?

The most important part of any web address (i.e. link) is the Domain. The domain is what comes right before the first single forward slash. When you hover your mouse over the link, always look for the actual domain. **Note:** Users with mobile devices should be aware that link hovering may not work. If the email is suspicious, wait to inspect it more closely from your PC and use the hovering technique.



If the part of the web address right before the first single forward slash (the Domain) is different than what you are expecting, the link could be malicious.

An example would be a web address of <http://support.amaz.on.com/onsale> where it may look like it goes to Amazon, but is actually going to the on.com domain. Always hover over a link to see the actual address. This technique also works on links within documents.

# Phishing Warning Signs

The image shows an email interface with the following content:

From: System Administrator<sysadmin@gmail.com> Sent: Mon 1/9/2017 1:11  
To: King, Stephen  
Cc:  
Subject: Email Account to be deactivated due to suspicious activity

Message: Untitled.skp (124 KB)

Dear User:

This email is to inform you that your email account has been deactivated by your Sys Admin due to unusual activity.

To reactivate your account please click on the following link.

[Reactivate Mailbox](#) [www.my-croperate.com/logmein](http://www.my-croperate.com/logmein)

Thank you,  
Sys Admin

If your mailbox remains deactivated longer than 5 days it will be deleted. Respond now to avoid.

Contact Support: 1-800-555-0100

Seven warning signs are indicated by red circles and arrows:

- 1 Emails sent from public email address (points to the sender's email address)
- 2 Unsolicited attachment (points to the 'Message' header)
- 3 Generic greetings (points to 'Dear User:')
- 4 Spelling mistakes (points to 'unusual' in the body text)
- 5 Links to unrecognized sites or slightly misspelled sites (points to the URL 'www.my-croperate.com/logmein')
- 6 Threat or enticements that create a sense of urgency (points to the yellow highlighted warning text)
- 7 Toll free numbers in suspicious emails that don't match known numbers (points to the phone number '1-800-555-0100')

# Victim of Identity Theft

## TAKE ACTION IMMEDIATELY!

- Use the ID Theft Affidavit at [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft)
  - Review recovery steps
  - Create a Personal Recovery Plan
- Contact your creditors and Follow up in writing
- Call where the fraud occurred
- File a complaint with the Federal Trade Commission
- Ask for verification that disputed accounts have been closed and fraudulent debts discharged
- File a police report



# Shared Responsibility

Security is the **shared** responsibility of your business and bank.

It takes a multi-layered approach from both.





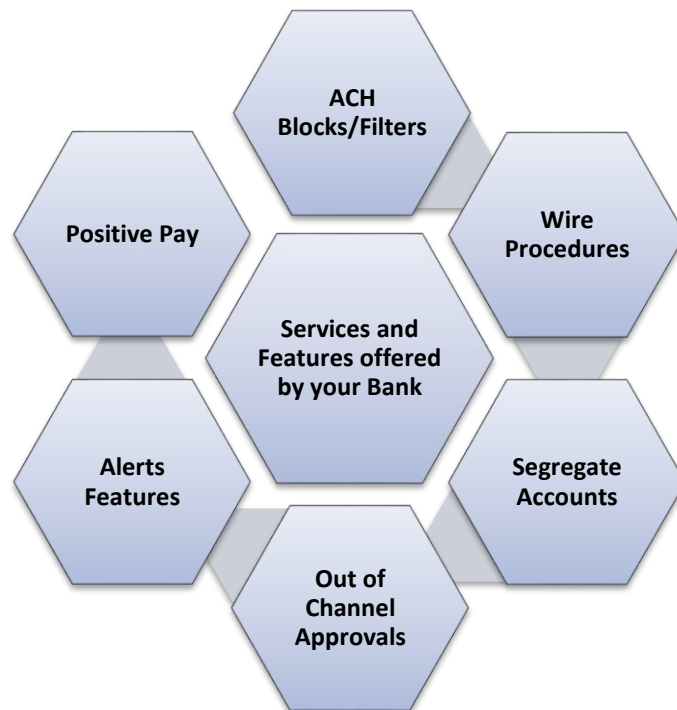
# Best Practice to protect your business

- Perform a risk assessment
- Establish company security policies and procedures
- Protect computer and mobile device endpoints (patch, anti-virus, etc.)
- Limit access and closely monitor accounts
- Train and test employees (awareness)
- Use a dedicated PC for high risk business functions (i.e. online banking)
- Use fraud detection and prevention tools for your bank accounts –  
ACH/ Check Positive Pay
- Consider commercial fraud insurance



# Protect – Best Practices in Fraud Prevention

Services available from your bank.



# Detect – develop and implement the appropriate activities

Daily	Review bank accounts daily
Reconcile	Reconcile all bank accounts
Audit	Regularly review online banking usage
Dedicated	Have a PC that is only utilized for banking
Rotate	Cross-train staff and rotate responsibilities
Beware	Prepare for 3-day weekends & sudden changes in business practices



Thank you!

Lucie Hannigan, SVP  
Treasury Management  
(207)828-3145  
[Lucie.Hannigan@peoples.com](mailto:Lucie.Hannigan@peoples.com)

Janet Butland, VP  
Market Manager  
(207)828-3036  
[Janet.butland@peoples.com](mailto:Janet.butland@peoples.com)