eCommercial SAT

eCommercial Security Awareness Training

Version 3.0

Welcome

The goal of this training course is to provide you with the information needed to assist in keeping your online banking account and transactions secure. Through education and awareness, you will have the ability to protect, detect, and respond to attempted breaches to your online accounts and transactions.

The course contains three sections:

Learning is a continuum; it starts with awareness, builds to training, and evolves into education. *

*National Institute of Standards and Technology NIST Special Publication 800-50

I. Basics of Commercial Online Banking Fraud

Online banking is a great technological convenience. Unfortunately, bad guys also known as cybercriminals target business accounts for monetary gain.

Our financial institution is pleased to provide education and raise the awareness of our business customers so that you can help prevent and detect fraud. The content in this course includes information that will assist in promoting your business's security environment, making it safer for online banking transactions.

Regulation E

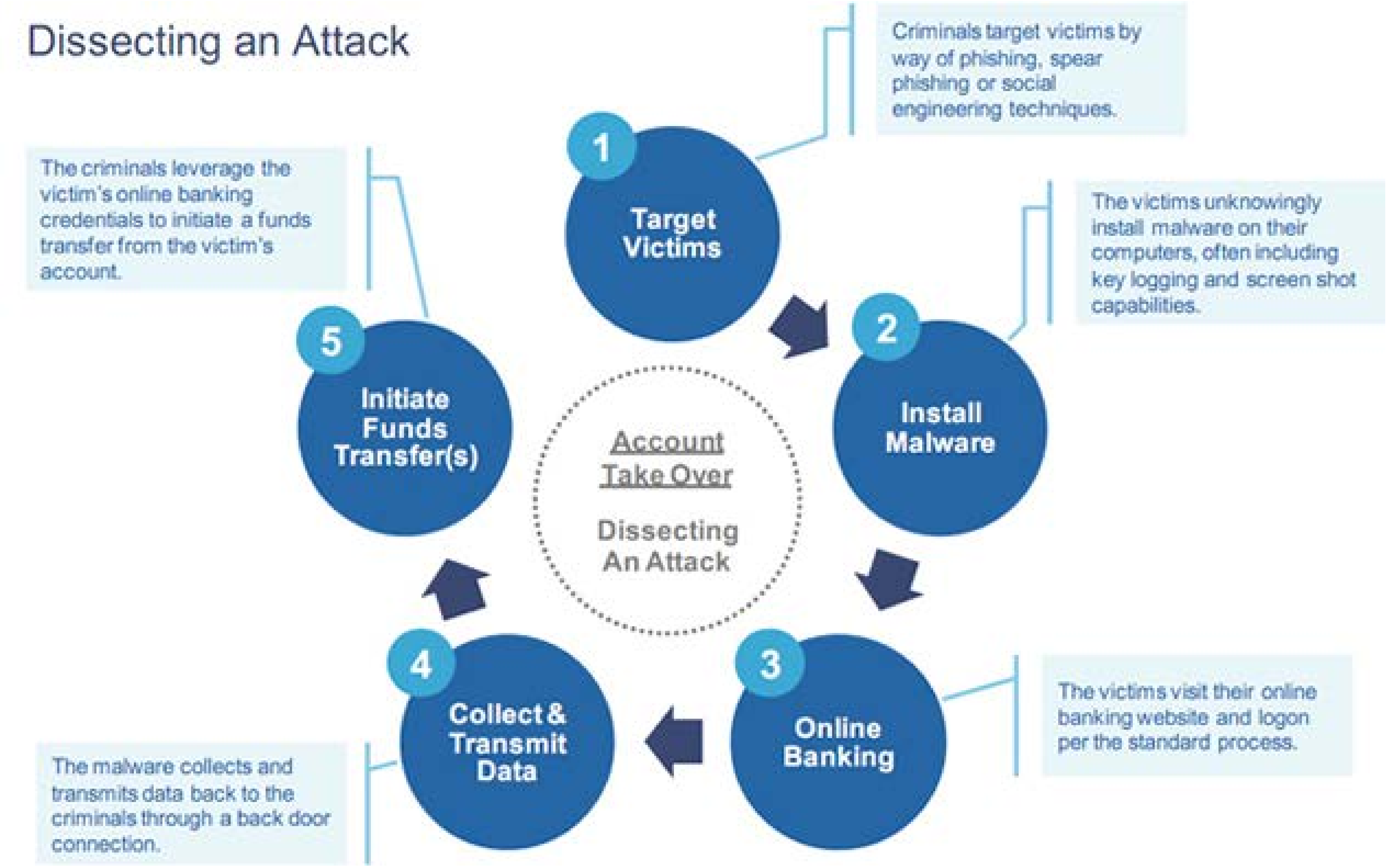
All businesses that conduct online banking transactions need to know about Regulation E.

Regulation E requires financial institutions to insure consumers and their accounts. **However, Regulation E does not include protections for commercial accounts.** Therefore, any protections afforded for fraudulent ACH or wire transactions made from your account(s) are addressed through our deposit account contract and/or state laws.

For more detail regarding Regulation E, see the *Regulation E - Business vs. Consumer Protections* document in Section 2 - Supporting Documents

Corporate Account Takeover

Online banking business accounts are attractive targets for cybercriminals. Cybercriminals use a scheme referred to as Corporate Account Takeover in order to commit online account fraud. See the breakdown of a common Corporate Account Takeover scenario below.



Criminals target victims by way of phishing, spear phishing or social engineering techniques.

The victims unknowingly install malware on their computers, often including key logging and screen shot capabilities.

The victims visit their online banking website and logon per the standard process.

The malware collects and transmits data back to the criminals through a back door connection.

The criminals leverage the victim's online banking credentials to initiate a funds transfer from the victim's account.

II. Threats and Controls to Online Transactions

The following section will provide information on how your business can prevent and recognize the signs of fraud.

For a comprehensive checklist of items to consider regarding your online security, see the *Commercial Online Banking Risk Assessment* in Section 2 - Supporting Documents

Back to the Table of Contents

⏮ ◀ ▶ ⏭

Computer Security

Enhance the security of your computer and network to protect against fraud by using items like spam filters, anti-virus software, anti-spyware software, and other protective software types from trusted sources. Keep protective software applications and operating systems current with the latest recommended security patches.

TIP:

A very effective security control to consider is using a dedicated computer for your business online banking transactions that has no other function. Lock it down from receiving email and do not use it for general web browsing.

Safe and Responsible Internet Surfing

Knowing about different types of Internet fraud will give you an advantage to avoid the pitfalls.

First, one should know about the arsenal that cyber criminals have to execute their crimes.

Malware – software that contains malicious code.

Spyware – a type of malware installed on a computer that collects information about users without their knowledge.

Computer Viruses – intrusive malware that carries out unwanted or damaging operations.

Back to the Table of Contents

▎◀◀ ▶▶▎

Man-in-the-Middle or Man-in-the-Browser Attacks (MIM/MIB)

These attacks occur when a cybercriminal inserts himself between the business customer and the financial institution and hijacks an online banking session. The fraudster covers up his actions by directing the business customer to a false website that looks like the authentic financial institution's website.

Watch out for messages that alert you that your online banking website is experiencing technical issues or is temporarily unavailable. This could be buying time for fraudsters to steal funds.

Call your financial institution immediately if you notice anything unusual or see suspicious messages during an online banking session.

The MIM/MIB scam often works in tandem with people who are known as Money Mules.

Man-in-the-Email

The **"man-in-the-email"** scam is a growing trend. This is when a legitimate email is intercepted by a fraudster before it reaches a businesse's inbox. Then a series of spoofed emails are launched in this scam, impersonating an established vendor. The email commonly uses the explanation that the vendor has a new FI account due to an audit. Businesses believe they are making payments to their vendors when in fact the funds are going to the cyberthief.

Tips to Mitigate this Scam:

- Establish other communication channels, such as a phone call to verify transactions.
- Always forward business emails to a known email contact instead of hitting reply.
- Carefully examine email purporting to be from vendors, especially if it appears to be outside of the usual pattern.

ATM Cash-Out Scheme

After thieves obtain access to FI online accounts they have hijacked, they divert money to fraudulent FI accounts as well as prepaid debit cards they contol. They then use hired crews known as "cashers" to withdraw funds from fraudulent accounts through ATM withdrawals and by making fraudulent purchases. Check your FI accounts each day to ensure that you are not seeing unauthorized transactions occur.

Email Phishing

Phishing is an attempt by an individual or group to solicit personal information from unsuspecting users by employing a technique known as social engineering. Phishing emails are crafted to appear as if they have been sent from a legitimate organization or someone you are familiar with (known as spear phishing).

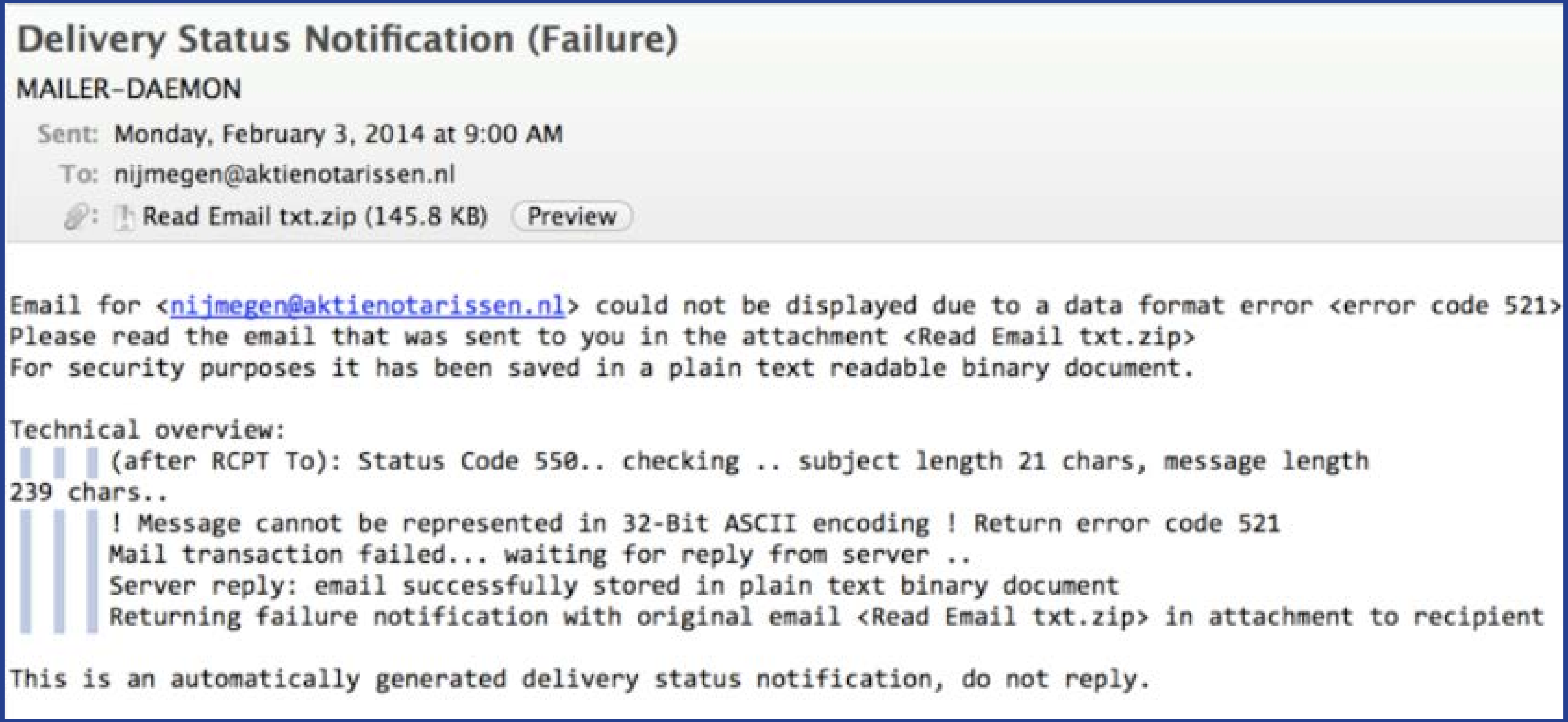
These emails often attempt to entice users to click on a link that will take the user to a fraudulent website that appears to be legitimate. The user may be asked to provide personal information such as account user names and passwords that can further expose them to future compromises. Additionally, these fraudulent websites may contain malware*

*Definition from US-CERT , Report Phishing Sites, Retrieved November 13,2012 from http://www.us-cert.gov/nav/report_phishing.html

The following pages will provide examples of phishing emails. Review these for signs to avoid.

|◀◀ ▶▶|

Phishing Example - Delivery Status Notification



Delivery Status Notification (Failure)

MAILER-DAEMON

Sent: Monday, February 3, 2014 at 9:00 AM

To: nijmegen@aktienotarissen.nl

Read Email txt.zip (145.8 KB)

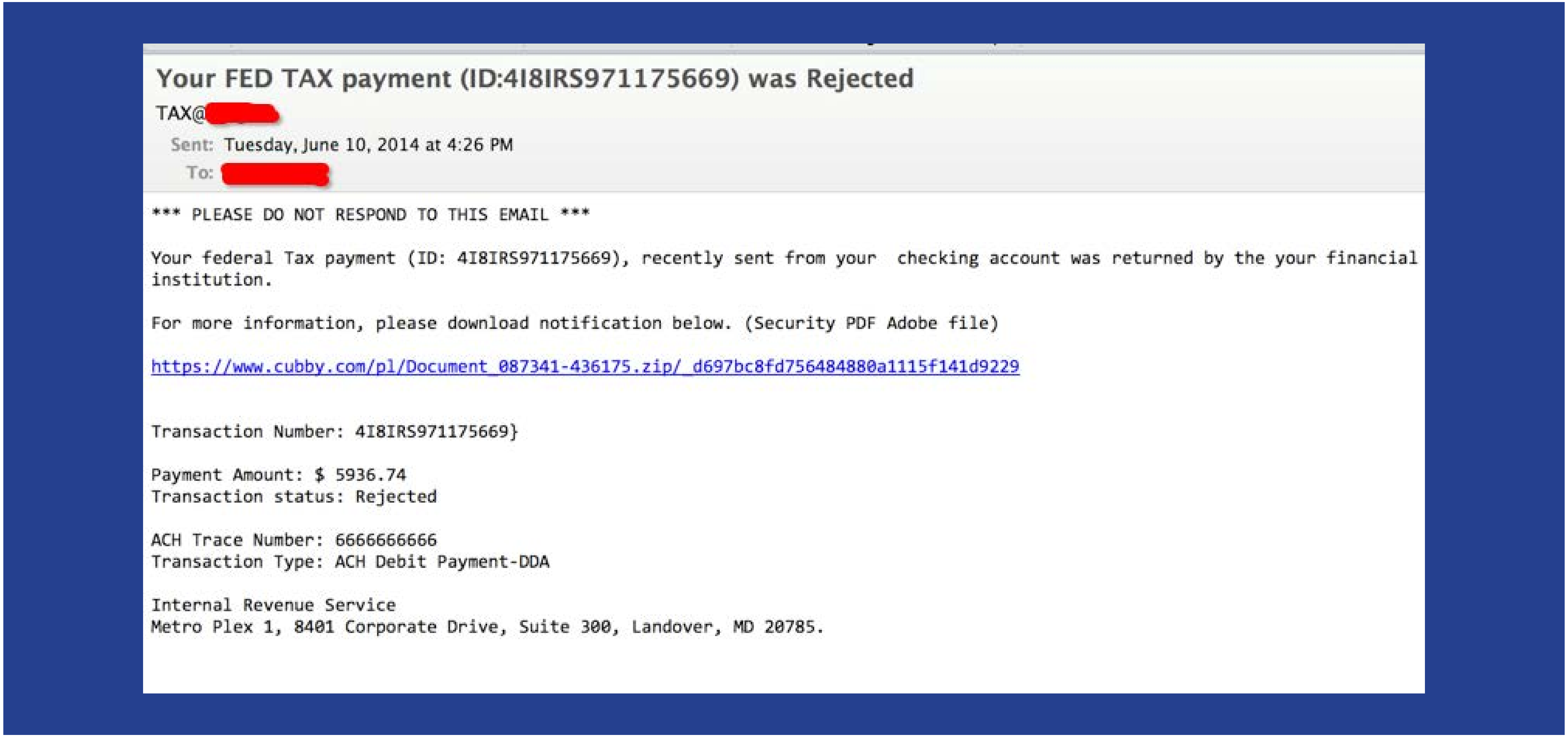
```
Email for <nijmegen@aktienotarissen.nl> could not be displayed due to a data format error <error code 521>
Please read the email that was sent to you in the attachment <Read Email txt.zip>
For security purposes it has been saved in a plain text readable binary document.

Technical overview:
| | | (after RCPT To): Status Code 550.. checking .. subject length 21 chars, message length
239 chars..
| | | ! Message cannot be represented in 32-Bit ASCII encoding ! Return error code 521
| | | Mail transaction failed... waiting for reply from server ..
| | | Server reply: email successfully stored in plain text binary document
| | | Returning failure notification with original email <Read Email txt.zip> in attachment to recipient

This is an automatically generated delivery status notification, do not reply.
```

This phishing example attempts to trick recipients into thinking they sent an email that was not delivered. Notice the attached zip file titled, "Read Email txt.zip". If the zip file is opened, the computer will become infected with malware called "ransomware" that asks the user to pay a ransom.

Phishing Example - Federal Tax Payments



Your FED TAX payment (ID:4I8IRS971175669) was Rejected

TAX@[redacted]

Sent: Tuesday, June 10, 2014 at 4:26 PM
To: [redacted]

*** PLEASE DO NOT RESPOND TO THIS EMAIL ***

Your federal Tax payment (ID: 4I8IRS971175669), recently sent from your checking account was returned by the your financial institution.

For more information, please download notification below. (Security PDF Adobe file)

https://www.cubby.com/pl/Document_087341-436175.zip/_d697bc8fd756484880a1115f141d9229

Transaction Number: 4I8IRS971175669}

Payment Amount: $ 5936.74
Transaction status: Rejected

ACH Trace Number: 6666666666
Transaction Type: ACH Debit Payment-DDA

Internal Revenue Service
Metro Plex 1, 8401 Corporate Drive, Suite 300, Landover, MD 20785.

This is a common phishing scam that targets businesses. It directs the recipient to a link to learn more about a failed tax payment. Clicking on the link within the email will install malware on the user's computer that targets their private FI information in order to commit account fraud.

File Sharing Software

Use discretion with in-the-cloud file sharing software apps like the following examples:

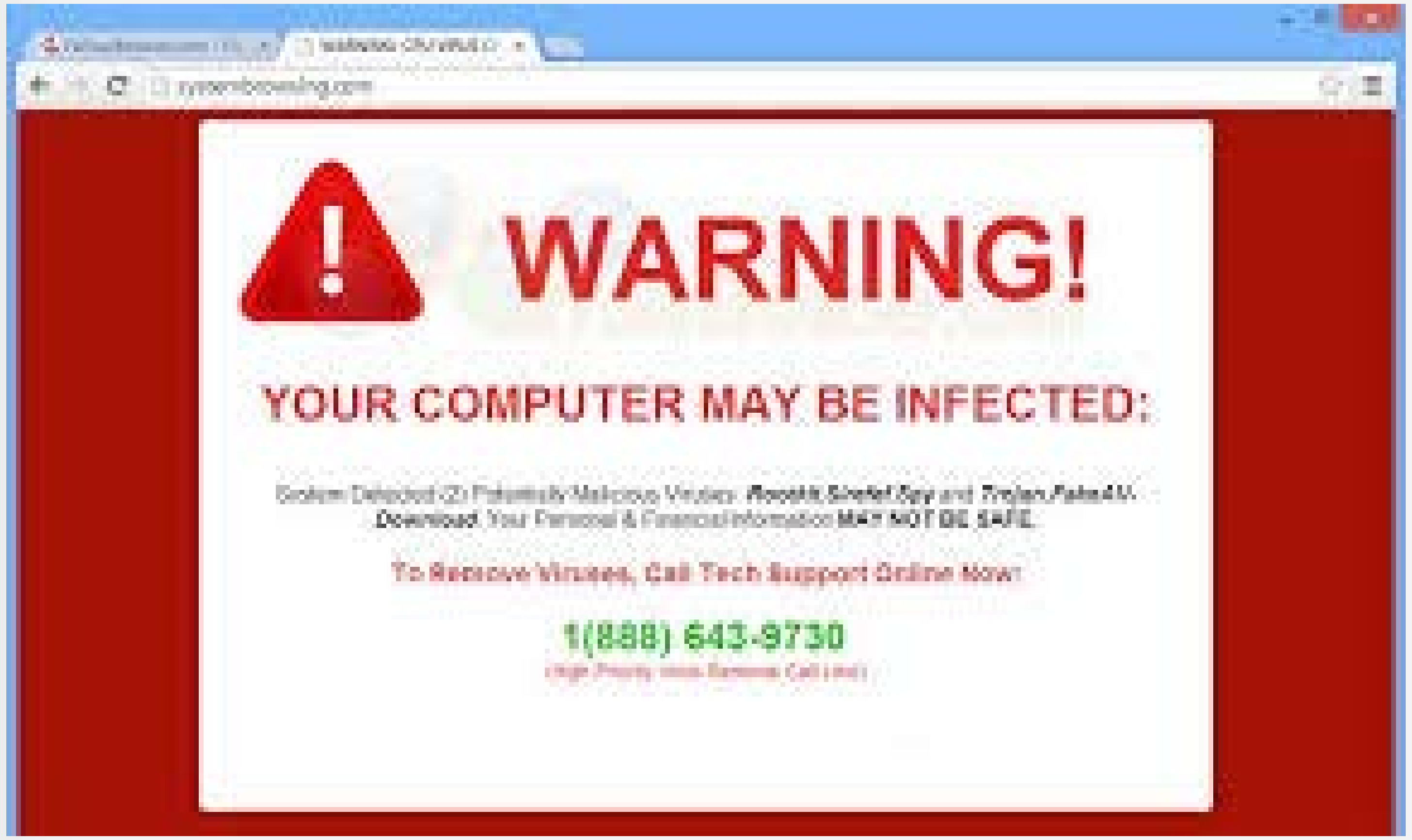
- Dropbox
- ICloud
- Google Drive
- BitTorrent
- SureSync
- GoodSync

These sites have potential vulnerability issues and given the right circumstances, a fraudster can install malware that may lead to a compromise of your computer and access to your online banking password account. It is not recommended to have this software on the same computer you use for online banking.

Pop-Ups/Fake Anti-Virus Scam

Be wary of pop-up advertisements, especially those claiming your machine is infected with a virus. This common scam will purport that it can fix your issue if you download and install the software. Once you install it, this malware can steal your online banking information.

Example:



WARNING!

YOUR COMPUTER MAY BE INFECTED:

System Detected (2) Potentially Malicious Viruses: *Rootkit.Sirefef.Spy* and *Trojan.FakeAV-Download*. Your Personal & Financial information **MAY NOT BE SAFE.**

To Remove Viruses, Call Tech Support Online Now:

1(888) 643-9730

(High Priority Virus Removal Call Line)

Mobile Device Security

Mobile devices such as smartphones, laptops, or tablet computers are as susceptible to threats as desktop computers. For example, malware infects mobile devices the same way as PCs, through a malicious email attachment. Be cautious regarding unsolicited mobile email. Criminals may send malware through text or email which could launch into an **overlay** attack. Overlay attacks appear to the user to be a standard online banking site's login page. However, the site captures the user's credentials in order to steal funds.

Unique threats to mobile devices include the following:

Mobile Malware – Malicious software aimed at mobile devices.

Smishing – Phishing scams that occur via text messaging. Clicking on unsolicited texts or photos sent to the mobile device may open up account holders for compromise to their accounts. This is especially an issue if you are using the device for anything related to your financial institution.

Easily Lost or Stolen – Password-protect your device and investigate capabilities for remotely wiping information from the device should it be lost or stolen.

Spear Phishing Goes Mobile - Fraudsters are increasingly gathering information about mobile and online users through groups they are affiliated with, as well as social media channels. One example is a scam targeting Android users, asking them to download a program on their device. The user downloads malware instead that collects storedinformation. Be careful about the kinds of information saved to a mobile device which can assist fraudsters in their efforts.

Mobile Device Tips

- Use the keypad lock or phone lock function on your mobile device when it is not in use. These functions password-protect your device so that nobody else can use it or view your information. Also, be sure to store your device in a secure location.

- Frequently delete text messages from your financial institution, especially before loaning out, discarding, or selling your mobile device.

- Never disclose via text message any personal information (account numbers, passwords, or any combination of sensitive information like your social security number or birth date that could be used in identity theft).

- Text banking users, if you lose your mobile device or change your mobile phone number, remove the old number from your mobile banking profile with your financial institution and contact customer service at your institution.

- Always read and follow instructions and guidance from your financial institution regarding securing your mobile banking experience.

- Turn off features of the device not needed to minimize the attack surface of the device.

Social Media Communication Security

Social Media Communication (SMC) sites are various online tools that enable people to communicate easily via the Internet to share information. However, if you use these sites on the same machine you use to conduct online banking transactions, you may be putting yourself at risk for online account fraud.

Examples of Social Media Communication or SMC sites:

- Facebook
- MySpace
- Twitter
- LinkedIn
- FourSquare
- YouTube
- Pinterest
- Google+
- Tumblr
- Flickr
- Second Life
- FarmVille and CityVille

Social media sites, such as Facebook and LinkedIn, can be used to determine who works at a particular company. Malicious users could use this information to develop spear phishing email attacks against an organization, in which narrowly targeted, malicious emails are crafted to seem authentic.*

*Common Sense Guide to Mitigating Insider Threats 4th Edition, Retrieved January 12th, 2014 from http://resources.sei.cmu.edu

Wireless Networks

Do you use the Internet at coffee shops or other places of business?

Be cautious when using public Internet services. There may be criminals looking at your online activity hoping to gain information about you. Avoid "listening outposts" used by hackers to trick you into giving up your sensitive login/password information. Check the connection types available. Beware of networks labeled "Free Wi-Fi network" or other similar "free" networked names. These wireless connections harvest your information once you log on to it and access sites. The have no encryption and no passwords are required.* This is not a secure means for conducting your online banking. There are certain types of malware that only target Wi-Fi access points. The bad guys sitting nearby could be hacking your session and collecting NPI (which is also called "being sniffed"). Refrain from accessing your online account via wireless or public access networks.

*http://www.ereviewguide.com/forums/networks-networking/918-wireless-networks-security-guide-protect-your-wifi-connection-hackers.html

Guarding Against Social Engineering

Here are some ways your business can defend itself against social engineering tactics:

- Limit details disclosed on any "Out of office" email messages. This information can be used for social engineering fraud.
- Be suspicious of unsolicited phone calls asking about employees or information about the business.
- Lock up any sensitive data in unattended areas.
- Shred sensitive documents. Do not throw them out in a disposal bin.
- Do not leave an unattended computer unlocked.
- Be suspicious. A social engineer preys on a person's willingness to be helpful.
- Use caution if answering questions on topics you didn't initiate. Criminals may pretend to be responding to your "request for help" in order to gain information. If you didn't ask a question, ignore the email, phone call, or text inquiry.

I◀◀ ▶▶I

USB Drives

Criminals are always finding new ways to get malware onto your computer. One way to do it is by piggybacking on USB drives. Inserting a compromised USB drive can transfer malware onto your computer.

How It Works:

An attacker might infect a computer with malware that can detect when a USB drive is plugged into a computer. The malware then downloads malicious code onto the drive. When the USB drive is plugged into another computer, the malware infects that computer. Some attackers have also targeted electronic devices directly, infecting items such as electronic picture frames and USB drives during production. When users buy the infected products and plug them into their computers, malware is installed.

Ways to Protect Your Data on USB Drives *

There are steps you can take to protect the data on your USB drive and on any computer that you might plug the drive into:

- Keep personal and business USB drives separate. Do not use personal USB drives on computers owned by your organization, and do not plug USB drives containing corporate information into your personal computer.

- Use and maintain security software, and keep all software up to date. Use a firewall, anti-virus software, and anti-spyware software to make your computer less vulnerable to attacks.

- Do not plug an unknown USB drive into your computer. Do not plug it into your computer to view the contents or to try to identify the owner.

* http://www.us-cert.gov/cas/tips/ST08-001.html

III. Responding to an Incident

Monitor and reconcile accounts at least once a day. This enhances the ability to quickly detect unauthorized activity and will assist in minimizing losses.

Pay attention to suspicious activity and react quickly. Look out for unexplained account or network activity, pop ups, and suspicious emails.*

Question: If you notice something out of place on your account or suspect that an incident has occurred, how do you respond?

Answer: If you believe there has been suspicious activity involving your online account, immediately contact us (by using the contact information located in the following section) so that we may take the appropriate actions.

The sooner you contact us, the better your chances are for preventing any financial losses.

* http://www.aba.com/Tools/Function/fraud/pages/corporateaccounttakeoversmallbusiness.aspx

Response Tips

- If you suspect your computer has been compromised, immediately cease activity on that machine.
- Disconnect the Internet cable and/or any other network connections (including wireless connections) to isolate the system from the network and prevent any unauthorized access.
- If possible, ask a computer support professional for assistance.
- Maintain a written chronology of what happened, what was lost, and the steps taken to report the incident.
- Have a contingency plan to recover systems suspected of compromise.

Basic Terms to Know

Computer Viruses - Intrusive malware that carries out unwanted or damaging operations.

Corporate Account Takeover - The act of cybercriminals gaining control of a business bank account and stealing a company's valid online banking credentials.

Cross Channel Fraud - Theft from deposit accounts by way of multiple points of access, whether branch, automated teller machine, call center, debit card, online banking, ACH, or wire.

Cybercriminals - Criminals who commit fraud through the Internet and computer networks.

Cyberthreats - Technical threats organized by cybercriminals attempting to gain unauthorized access and control of a computer through a network or data communications pathway.

Malware - Computer software that contains malicious code.

Money Mules - Money Mules are people who launder money for cybercriminals after they are either unwittingly hired for a bogus work-at-home job, or they knowingly take part in fraud for financial gain. Money Mules open an account, receive stolen funds into that account, and then wire the money out (usually overseas) for criminals to receive.

Operating Systems - An operating system, or OS, is a software program that enables the computer hardware to communicate and operate with the computer software.

Phishing - An attempt by an individual or group to solicit personal information from unsuspecting users by employing a technique known as social engineering.

Ransomware - Hijacks a user's computer by taking control of its monitor or screen, locking the system, and then displaying a ransom message. Typically, these messages appear to be from law enforcement agencies or some other trusted source such as a financial institution.

Social Engineering - The act of manipulating people into performing actions to release non-public information that they can use for identity theft.

Spear Phishing - A pinpoint attack against a subset of people (i.e., employees of a business) to attempt to undermine them. It will often look real and easily pass as an internal messages or a communication from a vendor. These emails often lure the end-user to a website, which will collect some form of sensitive information. Since the original email so closely mimics legitimate communications, end-users often do not hesitate to provide information such as login credentials.

Spyware – A type of malware installed on a computer that collects information about users without their knowledge.

Thank you for completing the Commercial Security Awareness Training.

We appreciate your business and want to work with you to protect your transactions. Being an informed and vigilant account holder, along with using our financial institution’s controls, will provide layers of security so that you can conduct online banking transactions with confidence.

Please close the browser window by clicking on the “x” in the upper right hand corner and proceed to Section 2 Supporting Learning Materials.