Cybersecurity Update

Dale Marroquin, CISSP
Information Security Officer
San Antonio Federal Credit Union

Topics

- Cybersecurity – news and headlines
- What are the threats and targets?
- Hackers and malware
- Email - Phishing
- Social Engineering
- Mobile device security
- Ways to protect yourself
- Questions

Cybersecurity Incident (1)

- **Washington Free Beacon website redirects to malware.**
  - Researchers found several pages on the Web site of the Washington Free Beacon were compromised and used to redirect users to a domain hosting the Fiesta exploit kit. The kit attempts to drop the ZeroAccess rootkit and the Internet Security Pro fake antivirus malware.

Cybersecurity Incident (2)

- **Researchers find self-propagating Zeus variant.**
  - Researchers at Trend Micro discovered a variant of the Zeus/Zbot trojan that spreads via a malicious .pdf file and then copies itself onto any removable drives detected on an infected computer

Cybersecurity Incident (3)

- **Apple Store vulnerable to XSS.**
  - A cross-site scripting (XSS) vulnerability was found in the Apple Store Web site, which exposes visitors to possible attack.

Cybersecurity Incident (4)

- **Mobile version of Cridex banking trojan spotted in the wild.**
  - A mobile version of the Cridex/Bugat banking trojan targeting Android, Blackberry, and Symbian devices was spotted in the wild by researchers from RSA.

Cybersecurity Incident (5)

The Cridex Trojan Targets 137 Financial Organizations in One Go

By Daniel Chechik • March 1st, 2012 • Botnets Cybercrime Malware Spam

A few weeks ago M86 Security Labs alerted that cybercriminals managed to compromise hundreds of WordPress-based sites. These attacks started with several large spam campaigns as reported in our most recent blog post on Cutwail. These emails included embedded URL links or HTML attachments that tricked the user to browse to the compromised Web sites. All these links eventually lead to Web pages infected with the Phoenix exploit kit. These cybercriminals operate Fast flux networks, which are a DNS technique used by botnets to hide the main C&C servers.

After the target machine is successfully exploited, the Phoenix exploit kit downloads a Trojan to the victim's machine. The downloaded Trojan is recognized by antivirus vendors under several names such as Cridex, Carberp and Dapato. Antivirus detection is quite low and only ten out of 43 antivirus scanners in VirusTotal can detect it.

Cybersecurity Incident (6)

- DDOS (distributed denial of service) attacks
  - Hacktivist group – Izz ad-Din al-Qassam Cyber Fighers (AQCF)
  - Overloaded organizations web servers
  - Focus was on financial institutions
    - University Federal CU in Austin – hit twice
  - Smoke screen for other attack channels

Cybersecurity Incident (7)

- **Microsoft and FBI storm ramparts of Citadel botnets.**
  - Microsoft and the FBI have disabled around 1,000 of the estimated 1,400 botnets created by the Citadel botnet malware that have stolen more than $500 million. Microsoft also filed suit against the alleged controller of the botnet, and the FBI is working with law enforcement in various countries to identify the botmaster and 81 bot herders

Source: FS-ISAC

Cybersecurity Incident (8)

- **Google researcher discloses zero-day exploit for Windows.**
  - A Google researcher discovered a security vulnerability in Windows that can be exploited to obtain administrator privileges, and has now published an exploit for the vulnerability

Source: FS-ISAC

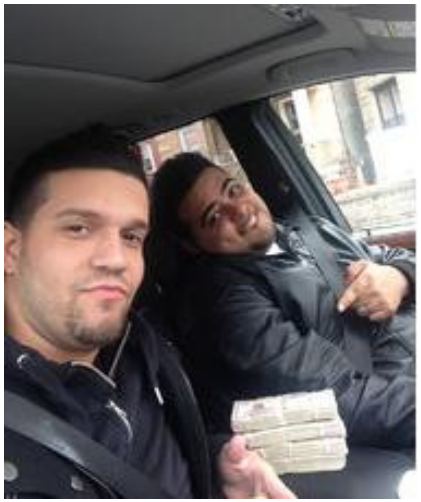
Cybersecurity Incident (9)

- **Red Robin customer's victims of months-long skimming scheme.**
  - A waitress who worked at a Red Robin restaurant in Des Moines, Washington, was arrested for allegedly skimming customers' credit and debit cards over several months, resulting in thousands of dollars in fraudulent purchases.

Source: FS-ISAC

Cybersecurity Incident (10)

- **Cyber thieves take $45 Million in ATM scheme**
  - In two precision operations that involved people in more than two dozen countries acting in close coordination and with surgical precision, thieves stole $45 million from thousands of A.T.M.'s in a matter of hours.



Cybersecurity Incident (11)

- **64% of data breaches caused by human and system errors, study finds.**
  - Symantec and the Ponemon Institute released their 2013 Cost of Data Breach Study that finds that 64 per cent of data breaches were due to human and system errors, among other findings.

Source: FS-ISAC

Cybersecurity Incident (12)

- **Anonymous member pleads guilty to Stratfor hack**.
  - A hacker who identified with the Anonymous hacktivist group pleaded guilty to participating in several attacks in 2010 and 2011, including attacks against law enforcement computer systems and global intelligence company Stratfor, based in Austin, Texas.

Cybersecurity Incident (13)

- Hackers Targeting industrial control systems
- Vulnerabilities in appliances running power plants, water treatment facilities, other critical infrastructure

Anonymous Hacker Group

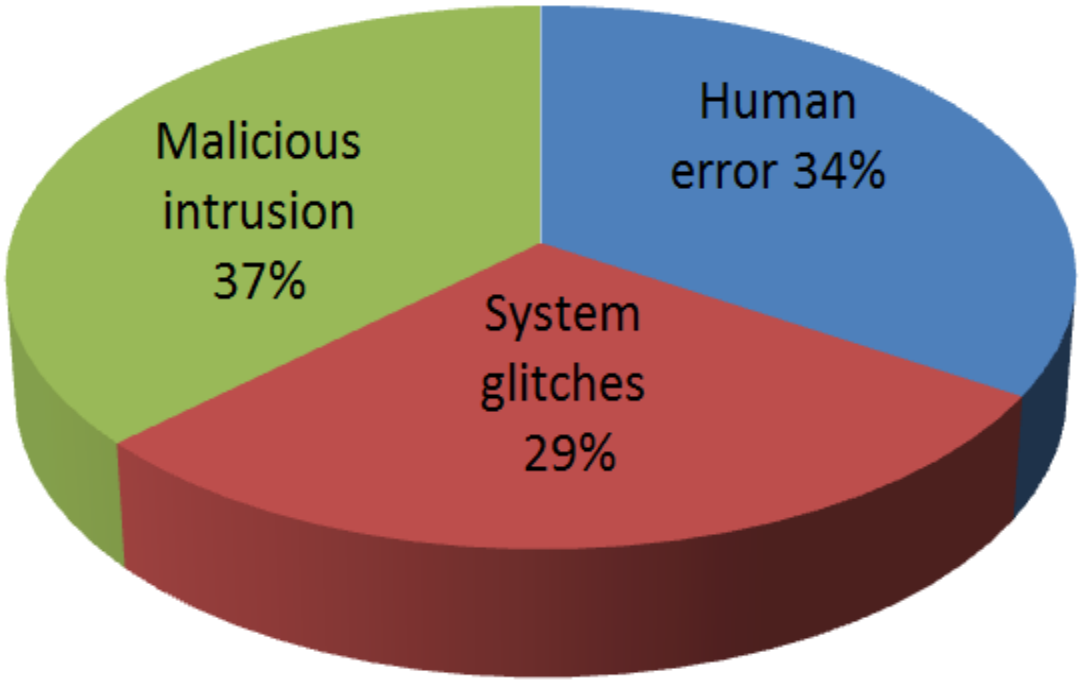
Anonymous Posts Names

- Posts file claiming to have information on 4,000 bank executives
- Data included personal and professional contact information
- Source of the data may have come from the Federal Reserve, which also acknowledged a hacker attack back in February this year

Cyber Attack Location of Origination

1. Xian, China
2. Wuhan, China
3. Fremont, California
4. Mumbai, India
5. Sao Paulo, Brazil
6. Santiago, Chile
7. Seoul, Korea
8. San Antonio, Texas
9. Taiyuan, China
10. Hamburg, Germany

Data Breach Causes



Source: Symantec and Ponemon

How Hackers have Evolved

- From script kiddies to organized crime
  - Identity theft
  - Financial fraud
  - Web site defacements
  - Data breaches
- Automated exploit kits
  - Blackhole
    - invisibly redirects to a compromised web site where malware is loaded
  - ZeroAccess rootkit
    - hides from detection software, secretly installing other malware such as blackhole. Can go undetected for months.

What is Malware?

- Short for “malicious software”
- Programming code designed to steal data
- It wants keystrokes, logins, passwords, credit card number, personal information
- Difficult to detect
- Hard to remove

What is a Botnet?

Not to be confused with a Beatnik

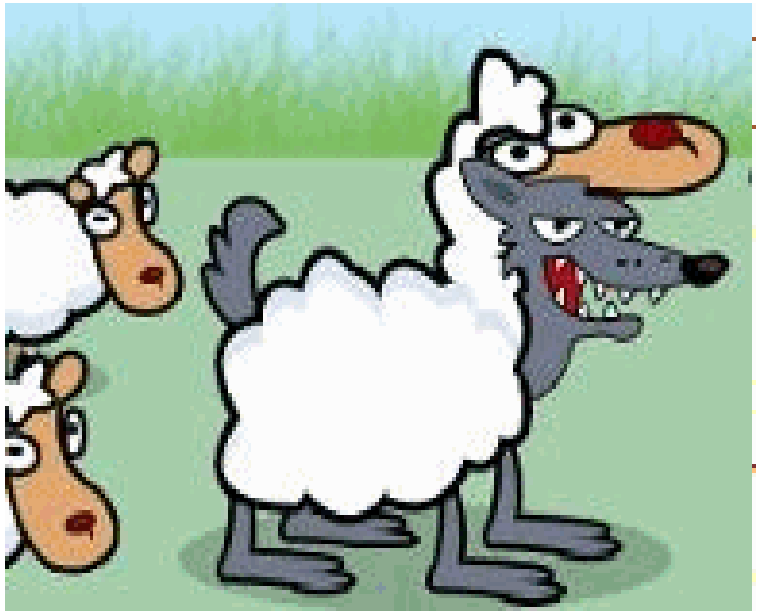
- Cultural group in the 50's and 60's
- Beat Generation
  - Sold books, swea bongos
  - Way of life that s ke dangerous fun
- Wore turtlenecks

Botnet

- A “bot” is type of malware that allows an attacker to take control over an infected computer
- A network of infected machines which operate as part of a “botnet”
- Machines exist across the Internet waiting on orders from their botmaster
- Capable of stealing sensitive information
- Can be used to launch denial of service attacks

Social Engineering

- The art of tricking someone by pretending to be someone they are not
- Manipulating someone into doing something they would not normally do
- The art of human hacking
- We are the weakest link



Social Engineering: The Scam

- The most common and current tactics:
  - Telephone calls
  - Email messages

Social Engineering Tactics

- “This is Microsoft support —we want to help“
- Charitable contribution scams
  - Donate to the hurricane recovery efforts!
- Any time there is a high-profile incident
  - Such as the devastating tornado’s or earthquakes
- Hackers are quick to launch fake contribution web sites.
- Initiate the contact yourself if you want to donate

The Dark Side of Email

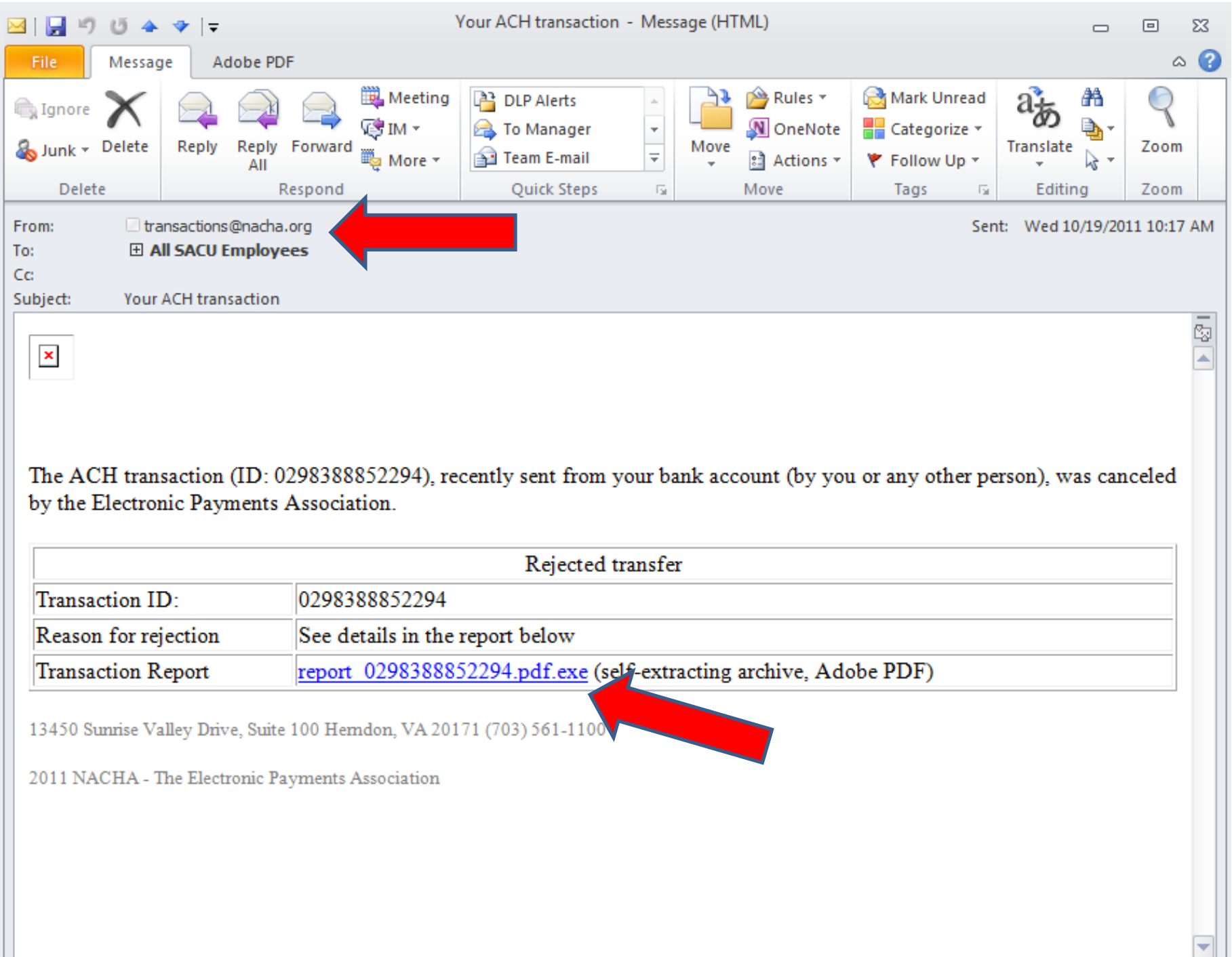
- SPAM
- Phishing
  - To good to be true
- Spear Phishing
  - Too true to be good
- Attachments
  - (.pdf, .exe)

Email Risks

- A few ways to detect:
  - Unknown sender
  - Sense of urgency
  - Unsolicited message
  - Foreign domain names
    - .ru = Russia
    - .co = China
- Delete from your Inbox
- Add them to your blocklist

Detecting Phishing Emails

- Appear to be from a trustworthy source
- Authentic looking – including logos
- Some have attachments
- Some have embedded links
- Try to lure you to:
  - Open the attachment
  - Click on the link
  - Install malware
- Usually sent in bulk distribution


Your ACH transaction - Message (HTML)
File
Message
Adobe PDF
Ignore
Junk
Delete
Reply
Reply All
Forward
Meeting
IM
More
DLP Alerts
To Manager
Team E-mail
Move
Rules
OneNote
Actions
Mark Unread
Categorize
Follow Up
Translate
Zoom
Delete
Respond
Quick Steps
Move
Tags
Editing
Zoom
From: transactions@nacha.org
To: All SACU Employees
Cc:
Subject: Your ACH transaction
Sent: Wed 10/19/2011 10:17 AM
The ACH transaction (ID: 0298388852294), recently sent from your bank account (by you or any other person), was canceled by the Electronic Payments Association.
Rejected transfer
Transaction ID: 0298388852294
Reason for rejection See details in the report below
Transaction Report report_0298388852294.pdf.exe (self-extracting archive, Adobe PDF)
13450 Sunrise Valley Drive, Suite 100 Herndon, VA 20171 (703) 561-1100
2011 NACHA - The Electronic Payments Association

Hallmark

e-cards from Hallmark

Someone has sent you a Hallmark E-Card.

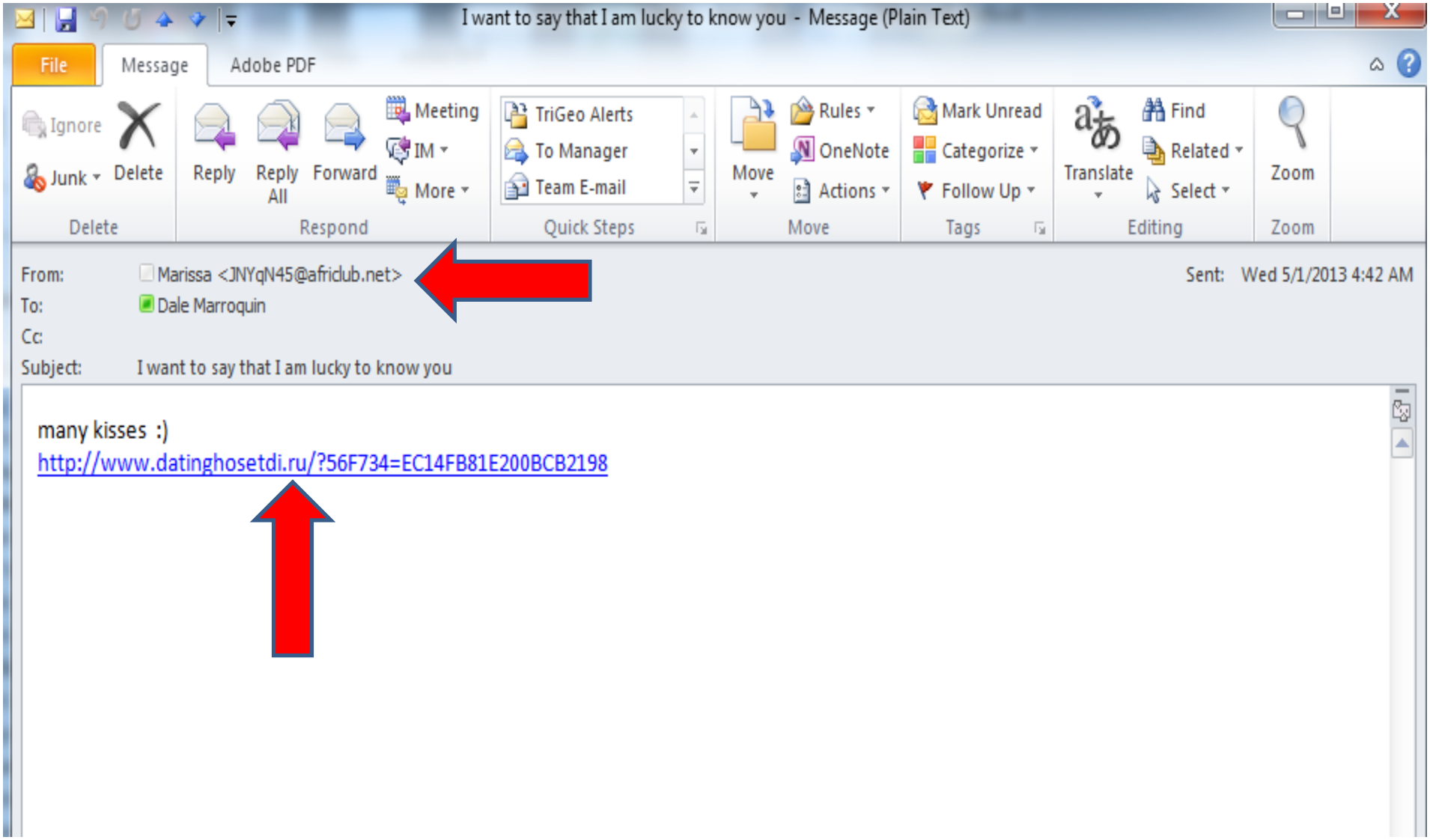
Simply click the link below to see your E-Card.
http://www.hallmark.com/ECardWeb/ECV.jsp?a=GRJ74JB43XLO9Z41G541&product_id=

If you have trouble using the link we provided, please follow these steps:

1. Visit http://www.hallmark.com/getecard
2. Enter your e-mail address in the Original Recipient's E-Mail Address box.
3. Enter GRJ74JB43XLO9Z41G541 in the Confirmation Number box.
4. Click Display Greeting.

Want to send an E-Card too ? Visit www.hallmark.com/ecards

HTTP://WWW.HALLMARK-E-CARD.COM/ECARD.HTML?ID=2098717867&BAE=905322749-904875494&MAILID=BAE_ECARD_ORDER&ID=EG2125-172139-81930940&USERID=0


I want to say that I am lucky to know you - Message (Plain Text)
File
Message
Adobe PDF
Ignore
Junk
Delete
Reply
Reply All
Forward
Meeting
IM
More
Respond
TriGeo Alerts
To Manager
Team E-mail
Quick Steps
Move
Rules
OneNote
Actions
Move
Mark Unread
Categorize
Follow Up
Tags
Translate
Find
Related
Select
Editing
Zoom
Zoom
From: Marissa <JNYqN45@afridlub.net>
Sent: Wed 5/1/2013 4:42 AM
To: Dale Marroquin
Cc:
Subject: I want to say that I am lucky to know you
many kisses :)
http://www.datinghosetdi.ru/?56F734=EC14FB81E200BCB2198

Dealing with Social Engineering

- Awareness is the number one defensive measure
- Inform your friends and family members
- Awareness that social engineering exists
- Awareness of the tactics most commonly used
- Changing behaviors is a ongoing challenge

Basic Security Controls and Safeguards

Things you can do

Tips on Passwords

- Use strong passwords
  - Upper, lower case, numbers, special characters
- Use a different passwords for different systems
  - Especially personal and business access
- Should never be stored in clear text
- Use password management software
  - 1Password, KeePass, or LastPass

Keep Systems Updated

- Apply vendor patches and updates
  - Not just operating system
  - 3rd party applications (Adobe, Java, Browser)
- Microsoft Black Tuesday
  - 2nd Tuesday of each month
- Use anti-virus / malware software
  - Keep definitions updated
  - Live update

Mobile Devices

- Smartphones, tablets are new attack vector

Mobile Device Security Tips (1/2)

- **Passcode**
  - Set a password on your mobile device so that if it is lost or stolen, your data is more difficult to access.
- **Trusted sources**
  - Only download apps from trusted sources, such as reputable app stores and download sites. Remember to look at the developer name, reviews, and ratings.
- **Pirated app?**
  - Use caution. Be wary of apps that offer a typically paid app for free, or an app that claims to install or download other apps for you.
- **Clicking on web links**
  - After clicking on a web link, pay close attention to the address to make sure it matches the website it claims to be, especially if you are asked to enter account or login information.

Mobile Device Security Tips (2/2)

- **Security app**
  - Download a mobile security app that scans every app you download for malware and spyware and can help you locate a lost or stolen device. For extra protection, make sure your security app can also protect from unsafe websites.
- **Check your phone bill**
  - Be alert for unusual behaviors on your phone, which could be a sign that it is infected. These behaviors may include unusual text messages, suspicious charges to the phone bill or suddenly decreased battery life.
- **Firmware updates**
  - Make sure to download and install firmware updates as soon as they are available for your device.

Attention Android Users

- Android malware cases to hit 1 million in 2013
- Android malware has grown at a faster pace in three years than was seen in PC-based malware in its first 14 years
- Google Play – formerly known as Android Market
- Lots of malicious apps

Security Apps for Androids and iPhones (1/2)

- **HiddenEye**
  - uses your smartphone's camera in self-defense: This app photographs any person who tries to unlock your phone.
  - *Available for:* Android *Cost:* Free
- **Find my iPhone**
  - If you misplace your iPhone, this app will let you use another iOS device to find it and protect your data. Locates the missing device on a map, plays a sound, displays a message, remotely locks the device and/or erases all the data on it.
  - *Available for:* iPhone *Cost:* Free
- **Plan B**
  - Plan B is a find-my-phone app that you download after you lose your phone. Described as a "last resort" to find a missing phone, it allows the user to locate a lost device using cell towers and GPS. On some phones, Plan B can switch on GPS automatically.
  - *Available for:* Android *Cost:* Free
- **Secure Folder PRO**
  - A private storage solution for photos, videos, contacts, notes, credit cards and passwords. Features secret website bookmarks and private navigation system without history tracking, a "decoy" storage area to trick nosy intruders, and encrypted storage for credit card and other data.
  - *Available for:* iPhone *Cost:* $1.99

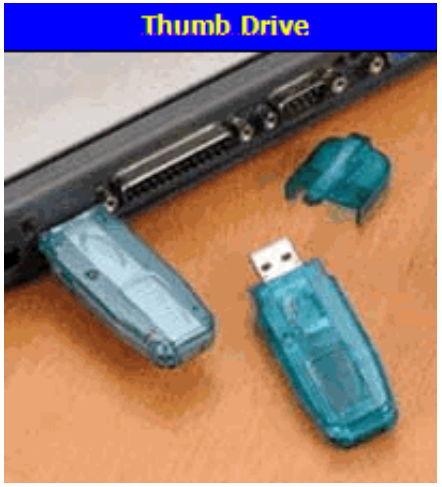
Security Apps for Androids and iPhones (2/2)

- **Lookout Mobile Security**
  - The Android version of this app includes antivirus; blocks malware, spyware and trojans; and scans each app downloaded. Both the Android and iPhone versions feature a find-my-phone component, which locates a lost or stolen phone on a Google map and activates a loud alarm, even if the device is set on "silent."
  - *Available for:* Android, limited version for iPhone *Cost:* Free
- **Norton Mobile Security**
  - Offers security, antivirus and antitheft protection. Includes automatic antivirus scan for downloaded apps and app updates, keystroke logging protection, remote lock and wipe, find-my-phone phone locator, and a "scream" locator that lets the user send a text to the missing phone, setting off a scream alarm.
  - *Available for:* Android *Cost:* Free
- **Privacy Filter**
  - Privacy Filter blocks the screen from prying eyes glancing at the device from the side.
  - *Available for:* Android *Cost:* $1.99

Social Networks

- Popular tactic – “Friend in Distress” scam
- Fake Facebook notifications – email message contains malware (keylogger)
- Be careful what you publish about yourself
  - Birthday, mother’s maiden name, graduation
  - Info can be used to guess your passwords
  - Info can be used in social engineering scam

The High Risk of a Low Cost USB device



- 1 out of 8 computer virus infections are made via USB device
- Most common carrier is a thumb drive
- Convenience, storage capacity and low cost make them popular to transport and store files
- USB safety tips:
  - Don't boot your PC with a USB device attached
    - Malware can be loaded directly to your PC ahead of some antivirus programs starting up
  - Run a virus scan on the device
  - Disable the “Auto-Run” feature in Windows
    - AutoRun can start an executable file that could potentially copy malware to your system
  - Spend a few dollars more for an encrypted drive

Internet Safety for Your Family (1/2)

- Windows Update set to automatic
  - www.windows.update.com
- Enable Windows Firewall
  - http://goo.gl/zqwGq
- Free home virus software
  - Avast – www.avast.com
  - AVG – free.avg.com
  - Avira – www.avira.com

Internet Safety for Your Family (2/2

- Microsoft Security Essentials
  - Windows.microsoft.com/mse
- Facebook Safety
  - http://fbparents.org
- Free anti-virus for Mobile Devices
  - Lookout Mobile Security – www.mylookout.com
  - Avast – http://avast.com/free-mobile-security

Mayhem = Malware?

Wrap Up

- Cyber security threat landscape continues to change
- Security is an evolving process
- Awareness is essential layer of protection

Thank you

Questions?