

Duke UNIVERSITY



HERUG 2016, April 11 - 14
Durham, North Carolina

Phished

What Happened and
What Was Done in
Response to a Targeted
Attack

Session T-3

Tedde Taege
Human Resources Lead
University of Nebraska

Learning Points

Background

What Happened?

Our Response

Our Solution

Conclusion



Learning Points

Background

What Happened?

Our Response

Our Solution

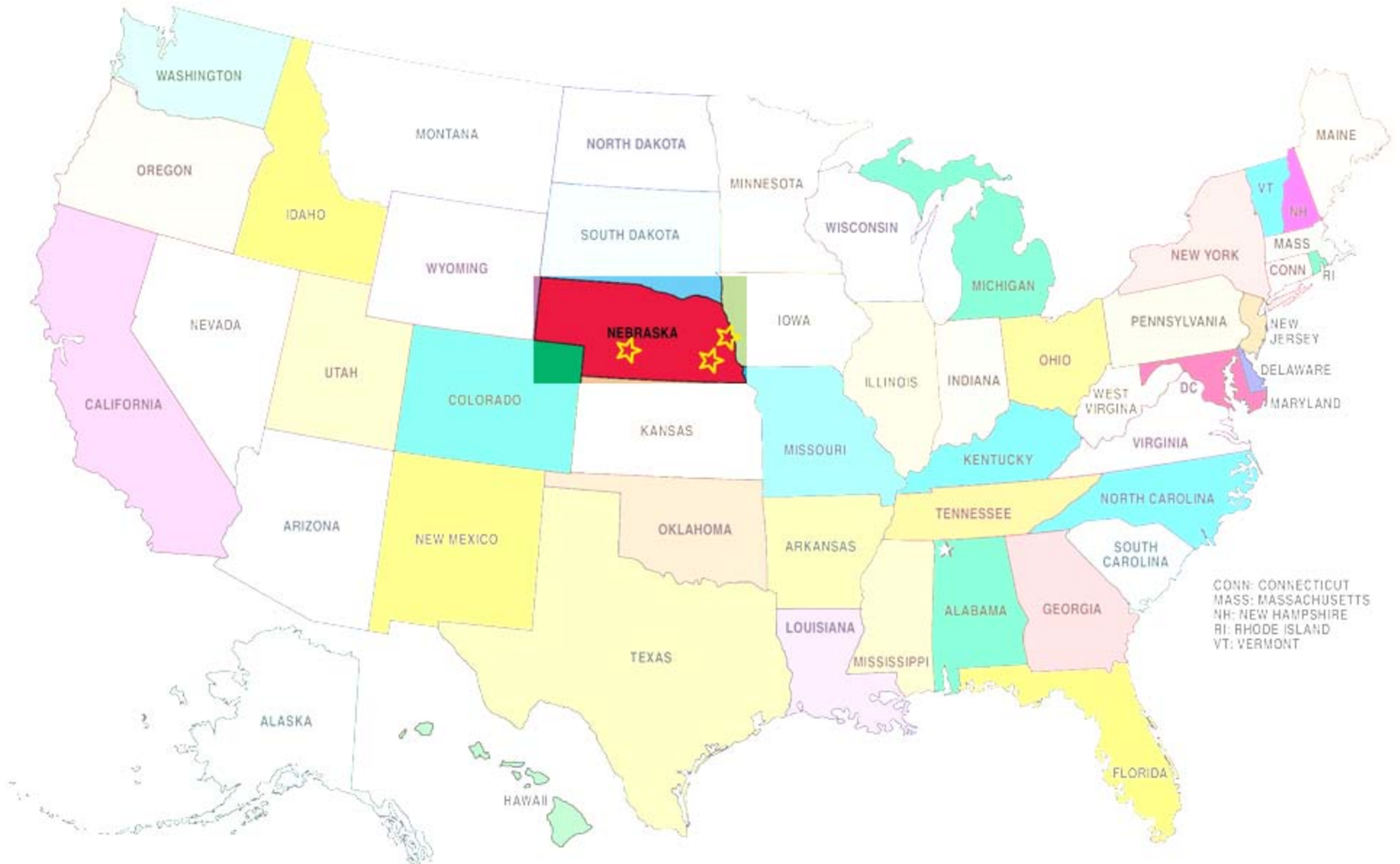
Conclusion



Background – University of Nebraska



- Four Campuses and University Central Administration
 - 51,000 Students
 - 12,500 Full-time employees
 - 14,500 Part-time employees
- Additionally...Our SAP installation also serves the Nebraska State College System
 - Three colleges
 - 807 Full-time employees
 - 2,075 Part-time employees



Background – SAP Installation

- Installed 1999 – Y2K Solution
- Modules / Applications
 - Finance (FI)
 - Accounts Payable (AP)
 - Accounts Receivable (AR)
 - Asset Account (AA)
 - Funds Management (FM)
 - Controlling (CO)
 - Cost Center Accounting
 - Materials Management (MM)
 - Purchasing
 - Inventory Management
 - Sales and Distribution (SD)
 - Business Intelligence (BI)
 - Human Resources (HR)
 - Payroll (PY)
 - Benefits
 - Organizational Management (OM)
 - Personnel Administration (PA)
 - Travel Management (TM)
 - Personnel Time Management (PT)
 - Project Systems (PS)
 - Project Costing
 - Enterprise Portal (EP)

What is the goal of information systems security?

- **Threat** – someone who wants your “stuff” without your permission.



- **Vulnerability** – a weakness which provides a vector into your information assets
- **Safeguard** – an effort meant to thwart a security threat. Could be hardware, software, or training.
- **Target** – the “stuff” that unauthorized people want.

What is Information Security

- **Information security** – a broad term encompassing the protection of information from accidental or intentional misuse by persons inside or outside an organization
- Organizations can implement information security lines of defense through people first and technology second



Unauthorized Data Disclosure Terms

- **Pretexting** – someone deceives by pretending to be someone else.
- **Phishing** – similar to pretexting except through email
 - **Spear phishing** – phishing directed at specific individuals
 - **Smishing** – combination of SMS texting and phishing
 - **Vishing** – combination of voice and phishing
 - **Whaling** – phishing attacks aimed a senior executives and high profile business targets
- “47 percent of adult Americans have been the victim of a breach in the last three years”
- “91 percent of the breaches we’ve see in the last few years have emanated from spear phishing.”
 - National Counterintelligence and Security Center Director Bill Evanina in 2015

What Are the Sources of Threats?

		Threat		
		Human Error	Computer Crime	Natural Disasters
Loss	Unauthorized data disclosure	Procedural mistakes	Pretexting Phishing Spoofing Sniffing Hacking	Disclosure during recovery
	Incorrect data modification	Procedural mistakes Incorrect procedures Ineffective accounting controls System errors	Hacking	Incorrect data recovery
	Faulty service	Procedural mistakes Development and installation errors	Usurpation	Service improperly restored
	Denial of service (DOS)	Accidents	DOS attacks	Service interruption
	Loss of infrastructure	Accidents	Theft Terrorist activity	Property loss

Learning Points

Background

What Happened?

Our Response

Our Solution

Conclusion



What Happened

- **Spear-phishing attack**
 - Employees tricked by a somewhat-believable e-mail message
 - Message crafted for NU campuses
 - Sent to a limited group of targeted people
 - Struck at an ideal time - right before weekends & holidays when systems are less monitored
- **Their Goal** – collect or modify information to steal money
 - Learn user IDs
 - Gather passwords
 - Discover social security numbers
 - Change bank account information

From: UNL RESOURCES <HREmployee payroll@unl.edu>

Date: September 5, 2015 11:18:14 AM CDT

To: [REDACTED]

Subject: Your September 2015 Paycheck

Date is a Saturday



Hello,

A letter confirming your salary raise starting September 2015 is hereby enclosed through your firefly account.

Login below to access this letter

[Access the documents here](#)

URL: <http://uldk.com/unl.edu/index.php>

***Ensure your login credentials are correct to avoid cancellations**

Faithfully

Human Resources

University of Nebraska^Lincoln

uldk.com/unl.edu/index.php

Firefly

User ID:

(e.g. NUID or UNMC NetID)

Password:

Social Security Number(SSN#):

[Need help logging in?](#)

LOGIN

Welcome to the Firefly Business Portal

Firefly provides easy and secure access to Employee and Manager Self Service Information, and so much more.



[Learn more about Firefly...](#)

Supported Browsers
Internet Explorer 9 thru 11
Mozilla Firefox Versions:
Extended Support Release
Rapid Release Current
Safari for Mac
Google Chrome

SAP

← → https://firefly.nebraska.edu/irj/portal/ University of Nebras... SAP NetWeaver Portal

Firefly

User ID:

(e.g. NUID or UNMC NetID)

Password:

[Need help logging in?](#)

LOGIN

Welcome to the Firefly Business Portal

Firefly provides easy and secure access to Employee and Manager Self Service Information, and so much more.



[Learn more about Firefly...](#)

Supported Browsers
Internet 11
Mozilla Firefox Versions:
Extended Support Release
Rapid Release Current
Safari for Mac
Google Chrome

SAP

Learning Points

Background

What Happened?

Our Response

Our Solution

Conclusion



How Did We Respond

- **Awareness**
 - Faculty forwarded phishing email to campus technical staff member on day received (Saturday)
 - Campus tech validated the spoofed website and passed the details off to central administration (CA) security analyst
- **Action**
 - CA security analyst requested that the website traffic be blocked via F5 hardware device (same day)
 - Check of access logs to see which users accessed the spoofed site from within our network (Sunday)
- **Impact**
 - Seventy-five emails phishing sent to UNL
 - Three users accessed site
 - One user logged into the site
 - User changed password (Tuesday)

How Did We Respond

By Friday of the attack week, we were ready to tell ourselves on “good job”

PHEW!!



BUT WAIT...

How Did We Respond

- **Assumed**

- We assumed that it was an isolated incident
- Failed to communicate to our other campus security contacts
- UNMC had a similar attack one week earlier and also did not communicate

From: UNMC-HR <xxx@unmc.edu>
Date: August 29, 2015 at 7:09:24 AM CDT
To: <xxx@unmc.edu>
Subject: Your New Paycheck As Adjusted

Right before Labor Day Weekend



Hello,

We assessed the 2015 salary structure as provided for under the terms of employment and discovered that you are due for a salary raise starting September 2015

Your salary raise documents are enclosed below:

<<< A link will be here >>>

Faithfully

Human Resources

University of Nebraska Medical Center

How Did We Respond

- **Damage**
 - User reported missing bank transfer from an outsourced flexible spending account
- **Re-Analyze the Situation**
 - Review of all banking changes for the prior three weeks
 - Thirteen users fell victim to the phishing email, logged into the fraudulent website, had compromised credentials, and banking information changed
 - Payroll staff and myself were reviewing potential impact and reverted one employee back to previous bank account at five minutes before our payroll final ran

Existing Safeguards

 Wed 4/6/2016 3:43 PM
SAPWorkflowUNP@nebraska.edu
Bank Information
To: [Redacted]

SAP Workflow

Bank Information

Your bank information has changed:
Please contact your payroll office immediately if you did not authorize this change.
Have questions about this email? Visit the [frequently asked questions](#) page.

 Wed 4/6/2016 3:44 PM
SAPWorkflowUNP@nebraska.edu
W-4 Notification
To: [Redacted]

SAP Workflow

W-4 Notification

W-4 Information:
Your W-4 tax withholding information has changed. Please contact your payroll office immediately if you did not authorize this change.
Have questions about this email? Visit the [frequently asked questions](#) page.

 Wed 4/6/2016 3:44 PM
SAPWorkflowUNP@nebraska.edu
Address Notification
To: [Redacted]

Bing Maps

SAP Workflow


Address Notification

Address Notification:
Your permanent address information has changed. Please contact your payroll office if you did not authorize this change.
Address changes can be reviewed in Firefly Employee Self Service (ESS). ***If this change impacts other addresses which are stored as part of your personnel record, the other addresses should be modified through ESS or by your payroll office.***
Modified Address: [Redacted]
Communications 1: [Redacted]
Communications 2: [Redacted]
Personal Email Address: unp@unp.net

Have questions about this email? Visit the [frequently asked questions](#) page.

Existing Safeguards

Firefly Security Verification □ ×



Security Verification
Enter the last four digits of your Social Security Number. XXX-XX-

REN-ISAC (Research and Education Networking Information Sharing and Analysis Center)

Suggestions To Defend Against Phishing Attacks

- Using two-factor authentication or virtual private network requirements
- Alerting users when direct deposit information has changed
- Redacting sensitive information available to the user in online systems to prevent the loss of additional personal information
- Implement systems to identify suspicious transactions in payroll systems, like as transactions routed to unusual geographic destinations or multiple users with the same account numbers
- Require additional information, like account details or a personal identification number

How Did We Respond

- **Review How Others Responded**
 - Numerous documented incidents of similar attacks
 - [Duke University](#) March 2014
 - [FBI Advisory](#) May 04, 2014
 - [Michigan State University](#) March 2014
 - [Nebraska Wesleyan University](#) June 2014
 - [Virginia Commonwealth University](#) June 28, 2014
 - [Longwood University](#) September 2014
 - [Washington University](#) September 20, 2014 & [01-23-2014](#)
 - [FBI PSA](#) University Employee Payroll Scam January 13, 2015
 - [University of Delaware](#) August 13, 2015
 - [University of Minnesota](#) August 28, 2015
 - [University of Chicago](#) November 2015
 - [University of Illinois](#) December 1, 2015 & July 2014

How Did We Respond

- **Review How Others Responded –**



- [Boston University](#)
- Shared their experience in an ASUG presentation
 - [Successful Phishing Attack Against Higher Ed](#) (8.26.14)
- Championed the concept of repeating existing bank account information before changing
- Created a banking audit report
- Implemented DUO two factor authentication

Learning Points

Background

What Happened?

Our Response

Our Solution

Conclusion



Our Solution

- **Retained our existing email notification and SSN verification**
- **User communication**
- **Required on-network access to change banking information**
- **Two factor identification to access network**
- **[Extended validation certificates](#)**
- **Banking information modification audit report**

Our Solution – User Communication

A targeted phishing attack on the University could have compromised your identity, bank information and email.

Direct deposits for payroll, travel and medical expenses may be at risk

In early September, a number of University employees received a fraudulent email asking for the entry of Firefly credentials. Some individuals were duped into responded to this email and revealed their credentials. The cyber criminals used that information to log on to Firefly and change banking information for those employees. They used that same information to log on to the individuals' email accounts and divert the system generated message that a bank account was changed.

That banking information provided governs the direct deposit of:

- Pay checks
- Travel reimbursements
- Flexible Spending Account deposits from WageWorks

This is no longer an advisory – you must protect yourself – the issue is real and it is here now!

If you have any suspicion that you may have inappropriately responded to such an email or that your credentials may have been compromised, please contact us at 402-472-7373 or servicedesk@nebraska.edu

To stay safe online and protect yourself against phishing, do the following:

Use a bookmark to access Firefly rather than clicking on a link in an email.

Do not click on links in unfamiliar emails.

Use different passwords for work and personal accounts.

Hover over links in emails before clicking on them to reveal their true destination.

Hover over the sender's name in Outlook to reveal the actual sender.

Walter

Walter Weir
Chief Information Officer
University of Nebraska

Our Solution – User Communication

Firefly News

A new article has been published on [Firefly's](#) Home page. Please read and distribute as necessary.

A targeted phishing attack on the University could have compromised your identity, bank information and email. Direct deposits for payroll, travel and medical expenses may be at risk.

Over the past few weeks, a number of University employees received emails with embedded website links to fraudulent websites asking for the entry of Firefly credentials. Some individuals were duped into responding to these requests and revealed their credentials. The cyber criminals used that information to log into to compromised Firefly accounts and change banking information for those employees.

Firefly banking information governs the direct deposit of:

- Paycheck
- Travel reimbursements
- Flexible Spending Account funds from WageWorks



This is no longer an advisory about good online behavior; it is real and it is here now!

If you have any suspicion that you may have inappropriately responded to such an email or that your credentials may have been compromised, please contact your campus Information Security Office immediately.

Our Solution – Require On-network Access

Our Solution – Two-Factor Identification

Two-factor authentication provides a second layer of security to any type of login, requiring extra information or a physical device to log in, in addition to your password.

The factors may include:

Something you know



a unique username and password

Something you have



a smartphone with an app to approve authentication requests

Something you are



biometrics - like your fingerprint or a retina scan

Our Solution – Two-Factor Identification

Two-Factor Methods

Hardware Tokens

Touching a physical device

Phone Callbacks

A phone call and a button press

SMS Passcodes

Passcode via text message

Mobile Passcodes

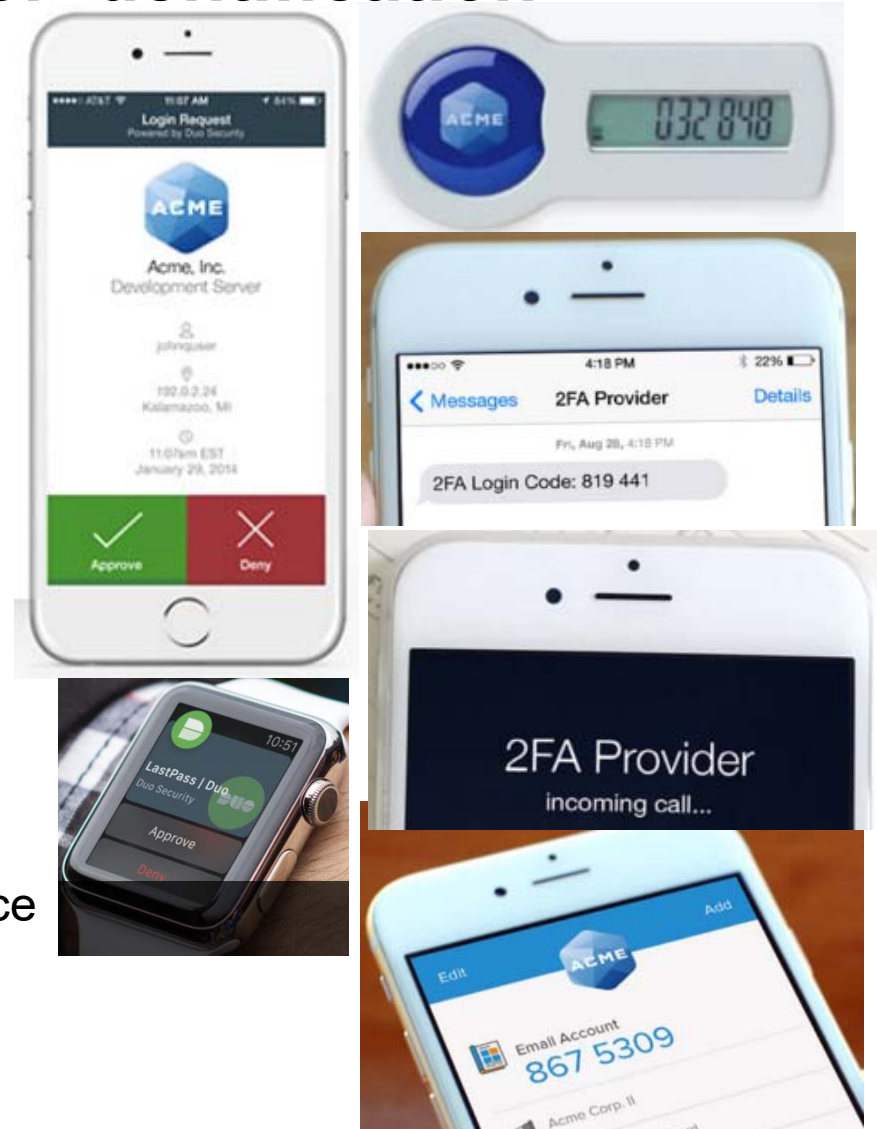
Passcode via two-factor app

Push Notifications

A push to your mobile device

Wearable

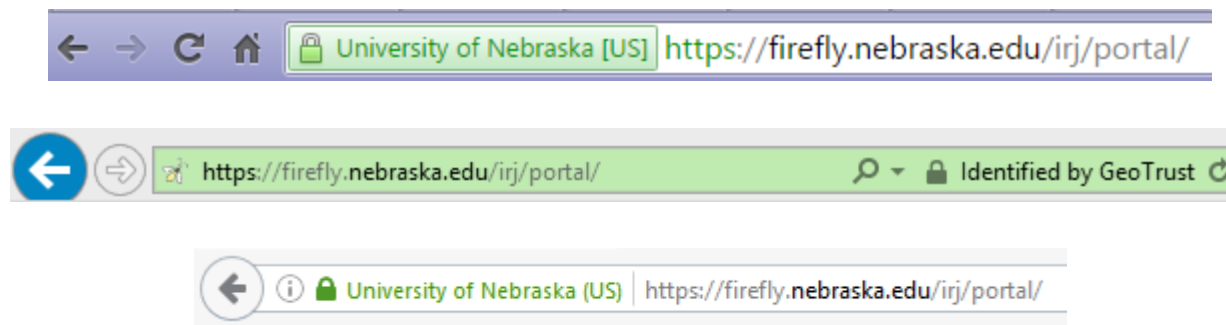
Passcode/Push/SMS via wearable device



Our Solution – Extended Validation Certificates

An Extended Validation Certificate (EV) is a public key certificate requiring verification of the requesting entity's identity by a certificate authority (CA).

EV certificates are mainly presented by web servers to web browsers for use with SSL/TLS connections. The certificates contain a subject with IDs for government entity, business category, or serial number presented in a way that a web browser can recognize the EV certificate.



Our Solution – Banking Information Modification Audit Report

UNIVERSITY OF NEBRASKA
USER: BATCH

BANKING CHANGE REGISTER
UNO

PAGE: 1
DATE: 04/01/2016
TIME: 00:31:59
SYS/CL: UNP 005

Name	Pernr	User ID	Chng by	Date	Time	Type	Action	Begin date	End date	Routing No	Bank Name	St	Account	C/S	Method
				03/31/2016	08:05:41	Main	CHGOLD	08/18/2006	03/24/2016	304083257	OMAHA POLICE FEDERAL CREDIT	NE	*5-A	S	DIRDEP
							CHGNEW	03/25/2016	12/31/9999	104000029	US BANK NA	MN	*034	C	
				03/31/2016	12:51:50	Main	CHGOLD	09/16/2011	03/31/2016	091408734	GREAT WESTERN BANK	SD	*628	C	DIRDEP
							CHGNEW	04/01/2016	12/31/9999	031101114	THEBANCORPCOM BANK	DE	*553		
				03/31/2016	07:55:24	Main	ADD	03/25/2016	12/31/9999	304083257	OMAHA POLICE FEDERAL CREDIT	NE	*340	C	DIRDEP
				03/31/2016	11:15:59	Main	ADD	04/04/2016	12/31/9999	104000854	AMERICAN NATIONAL BANK	NE	*877	C	DIRDEP

Learning Points

Background

What Happened?

Our Response

Our Solution

Conclusion



Conclusions

- **Educate the Weakest Link - Users**
 - Keep information in front of the users
- **Implement Multiple Safeguards**
 - Multiple levels of authentication
 - Notify users when critical information changes
 - Monitor system for banking information on multiple records
 - Monitor system for banking information modifications
 - Use hardware and software solutions to monitor web traffic and block unwanted traffic
 - Limit critical information access to “on-site” networks
 - Utilize two-factor authentication solutions

How to Recognize Phishing Scams

- Phishing attempts have become more sophisticated with increased quality of imitating a genuine email.
- Be aware of these warning signs:
 - Unsolicited messages asking you to update, confirm, or reveal personal identity information (e.g., SSN, account numbers, passwords, protected health information).
 - Message creates a sense of urgency.
 - Message has an unusual “From” address or an unusual “Reply-To” address.
 - Website URL (most likely malicious) doesn’t match the name of the institution that it allegedly represents.
 - Message is not personalized. Valid messages from banks and other legitimate sources usually refer to you by name.
 - Message contains grammatical errors.

Phishing Email Dos and Don'ts:

- **DO** call a company that you received a suspicious email from to see if it is legitimate, but **DO NOT** use the phone number contained in the email. Check a recent statement from the company to get a legitimate phone number.
- **DO** look for a digital signature/certificate as another level of assurance that senders are legitimate. Digitally signed messages will have a special image/icon at the subject.
- **DO** adjust your spam filters to protect against unwanted spam.
- **DO** use common sense. If you have any doubts, **DON'T** respond. Ask your department IT representative.

- **DON'T** open email that you have any suspicion may not be legitimate. If it is legitimate and the individual trying to contact you really needs to, they will try other means.
- **DON'T** ever send credit card or other sensitive information via email.
- **DON'T** click the link. Instead, phone the company or conduct an Internet search for the company's true web address.
- **DON'T** open email or attachments from unknown sources. Many viruses arrive as executable files that are harmless until you start running them.

How Should You Respond to Security Threats?

- Take security seriously
- Create strong passwords and use a unique password for each site <https://howsecureismypassword.net/>
- Do not send data via email or IM
- Clear browser history
- Regularly update antivirus software
- Follow organizational security directives



How Should Organizations Respond to Security Threats?

- Establish a company-wide security policy.
- Minimally should stipulate:
 - What sensitive data to store
 - How it will process that data
 - If data will be shared with other organizations
 - How employees and others can obtain copies of data stored about them
 - How employees and others can request changes to inaccurate data
 - What employees can do with own mobile devices at work
 - What non-organizational activities employees can take with employee-owned equipment



The First Line of Defense - People

- The biggest issue surrounding information security is not a technical issue, but a people issue
- 38% of security incidents originate within the organization
 - **Insiders**
 - **Social engineering**



The First Line of Defense - People

- The first line of defense an organization should follow to help combat insider issues is to develop information security policies and an information security plan
 - **Information security policies** – identify the rules required to maintain information security
 - **Information security plan** – details how an organization will implement the information security policies



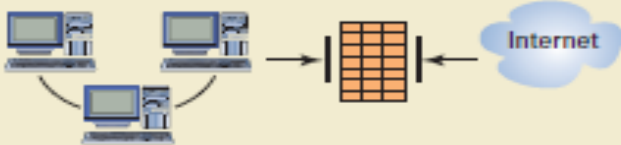
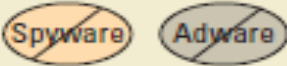



The Second Line of Defense - Technology

- Three primary information security areas
 1. Authentication and authorization
 2. Prevention and resistance
 3. Detection and response



How Can Technical Safeguards Protect Against Security Threats?

- Identification and authentication 
- Encryption 
- Firewalls 
- Malware protection 
- Design for secure applications 



How Can Data Safeguards Protect Against Security Threats?

- Define data policies
- Data rights and responsibilities
- Rights should be enforced by user accounts authenticated by passwords
- Data Encryption
- Backup and recovery procedures
- Physical security



How Should Organizations Respond to Security Incidents?

- Have a plan
- Plan should include centralized reporting
- Speed of response is critical
- Practice incidence response



Future?

- Future Cyber Crimes - <http://www.foxbusiness.com/personal-finance/2014/05/14/future-crime-8-cyber-crimes-to-expect-in-next-20-years/>
- Attacks more common, inflicting serious damage
- Security mobile devices improved
- Improved security procedures and employee training
- Criminals focus on less protected mid-sized and smaller organizations, and individuals
- Skimming - <http://krebsonsecurity.com/wp-content/uploads/2011/02/greenskimoff.jpg>, <http://knco.com/wp-content/uploads/2012/07/ATM-machine-phoney1.jpg>, http://www.antiskimmingeye.com/wp-content/uploads/2013/12/skimming_device_3.jpg, 1:58 http://www.youtube.com/watch?v=m3qK46L2b_c
- <http://www.police.wa.gov.au/LinkClick.aspx?fileticket=12Xph2DRuWw%3d&tabid=887> http://nerdbeach.com/ExistingContent/CardSkimmer_102411.jpg
- Electronic lawlessness by organized gangs
- Electronic sheriffs patrol electronic borders

Stuxnet: The Virus that Almost Started WW3 (3:29) - <http://www.youtube.com/watch?v=7g0pi4J8auQ>

Stuxnet on 60 Minutes (14:55) - <http://www.cbsnews.com/news/stuxnet-computer-worm-opens-new-era-of-warfare-04-06-2012/>

Future of Cyber Security (1:10) - http://www.youtube.com/watch?v=zoHMF_m_ato

The New Era of Organized Cybercrime - <http://www.dailydot.com/crime/organized-crime-cybercrime-obsolete/>

A cosmic background featuring a dense field of galaxies and stars. In the center, a bright, glowing sphere is visible, with the words "THE END" overlaid in large, white, stylized, block letters. The text is slanted and appears to be floating in space, partially obscuring the sphere behind it. The background is dark, with various colors of light from distant galaxies and stars, including yellow, orange, and blue.

THE
END

