

---

# Cybersecurity Awareness

---



for everything that counts®



Member FDIC

# The Day Before Tomorrow:

A Discussion On  
Cybercrime & Fraud



# July 1994

## St. Petersburg, Russia

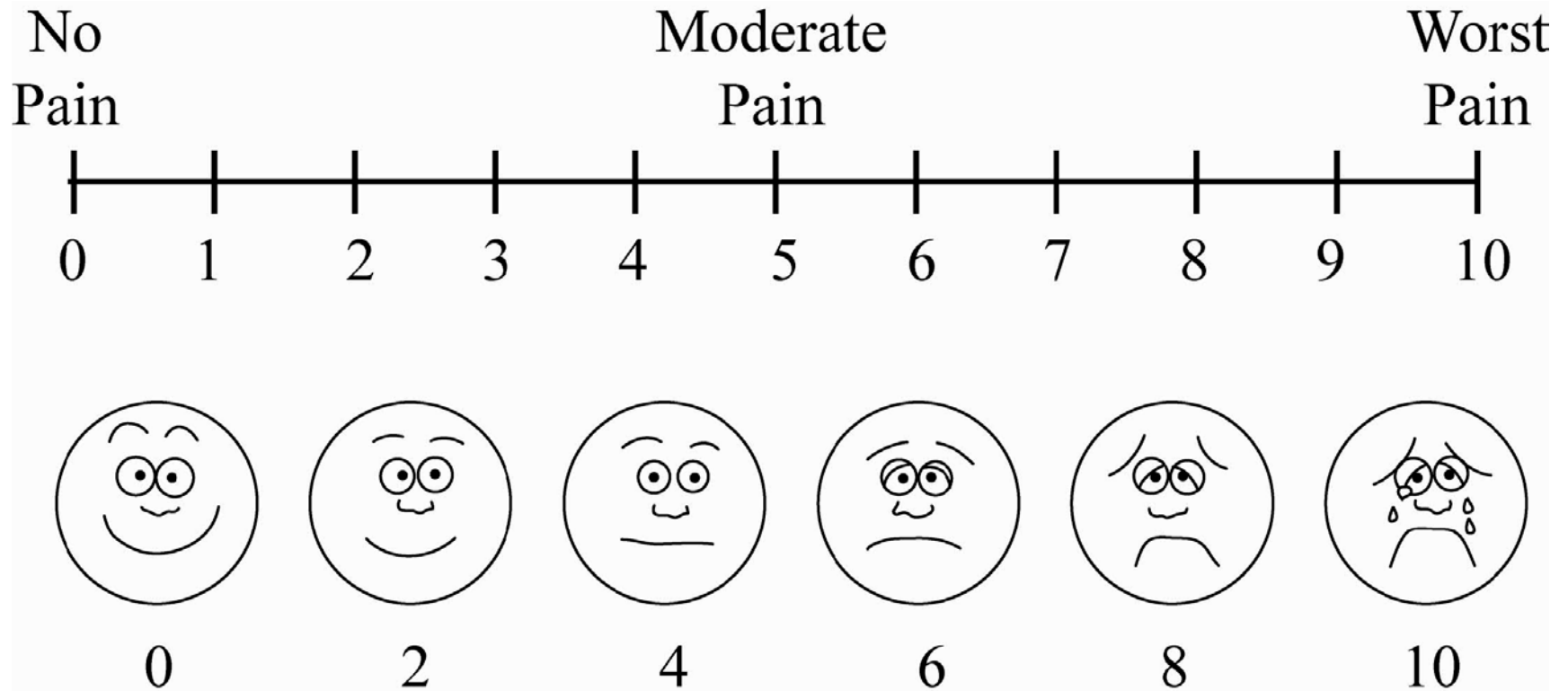


# Subject: Vladimir Levin

## Age: 23



# Cybercrime Pain Scale



# are you the lucky one?



# AGENDA

knowledge + tools > threats

4 case studies  
4 opportunities



# But First...

## Social Engineering Terms

- Phish
- Spoof
- Malware
- Keylogger
- pwn

# Case Study #1

What would you do differently **today**  
if you knew that tomorrow...

I **H**A V E Y O U R

n E **T** W O R K



p A **Y** U P O R **T** **H** E

d A **T** A **g** E **T** S I **T**

# Old "Past Due" Invoice Trick

dear sir,  
please click HERE and everything will be  
ok.  
ps i accept bitcoin

# What does being PWNED look like?

 Filenames redacted	.doc	4/26/2016 4:24 PM	DOC File	50 KB
	2013.doc	4/26/2016 4:24 PM	DOC File	49 KB
	.doc	4/26/2016 4:24 PM	DOC File	49 KB
	.doc	4/26/2016 4:24 PM	DOC File	46 KB
	2.doc	4/26/2016 4:24 PM	DOC File	42 KB
	oc	4/26/2016 4:24 PM	DOC File	46 KB
		4/26/2016 4:24 PM	DOC File	30 KB
		4/26/2016 4:24 PM	DOC File	30 KB
	ley.doc	4/26/2016 4:24 PM	DOC File	40 KB
	README-Encrypted_Files.HTML	4/26/2016 4:24 PM	HTML Document	4 KB

# Ransomware Preparation

- Anti-Virus
- Back-Ups
- Macros
- Table-Tops

# Case Study #2

What would you do differently **today**  
if you knew that tomorrow...

Your employee  
will drop you a **note**...

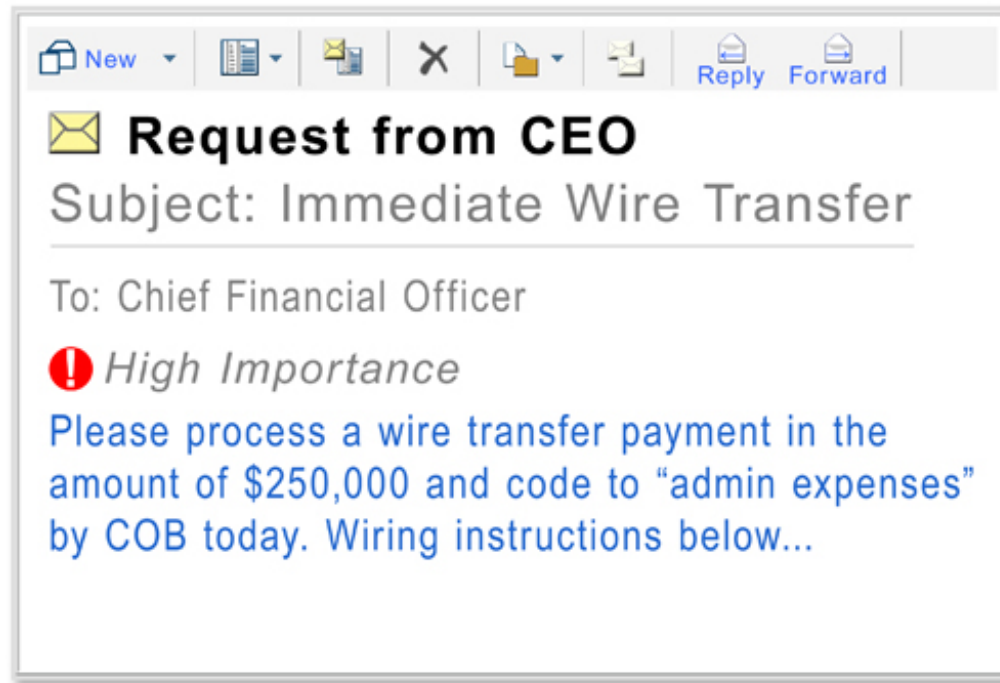
Hey Boss,

I wired that \$35,000 to  
crazyQ paper like you asked!  
Bank confirmed all set –

Cheers!

or worse,

**YOU** are that employee.



# Business Email Compromise (BEC)

the  
**\$2 BILLION**  
problem

# BEC Preparation

- @Consistency
- Dual Control
- Training
- Human Voice

# Case Study #3

What would you do differently **today**  
if you knew that tomorrow...



your *CHECKS* will  
be counterfeited

# The Signal



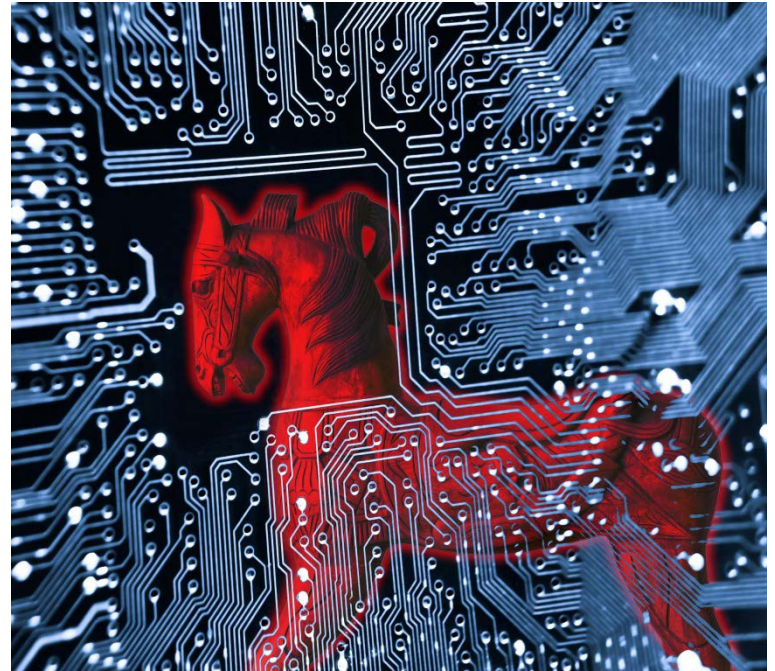
# Low-Tech & Successful

- Security
- Positive Pay
- Direct Deposit
- ACH Block

# Case Study #4

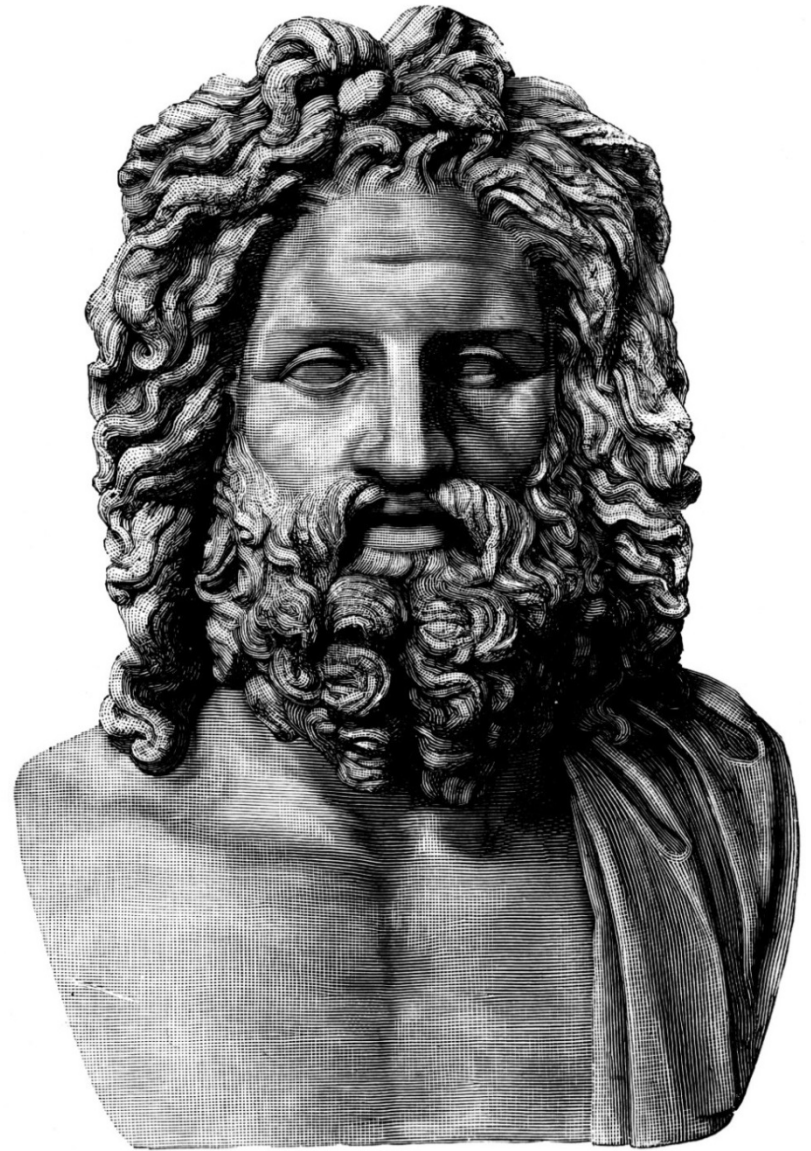
What would you do differently **today**  
if you knew that tomorrow...

Your bank  
calls to confirm  
a \$42,500 **ACH**  
payroll file,



and you **didn't** do payroll YET.

There is no  
school like  
**old** school.



# Account Takeover

- Reduce Threat Surface
- Dual Control
- Computer Security
- Training


# Epilogue





the 80s are over





It's *organized*,  
and it's just  
business.

1200 USD

click to order



where to **begin?**



# Cyber Insurance

for when the  
unthinkable  
occurs...



# Resources

## Fraud Information Center on NBT Bank's New Website



[Business](#) > [Customer Support](#) > [Fraud Information Center](#)

### FRAUD INFORMATION CENTER

For businesses of all sizes, incidents of fraud and theft of financial data are on the rise. Knowing this, few things count more to your business than securing your business's account information, and NBT Bank is committed to helping you do just that. Click the boxes below for the latest information, tips and resources related to business fraud.



Ransomware: Prevent, Detect, Respond [Learn More](#)



Be aware of the CEO Phishing Scam [Learn More](#)



# Resources

## Email & Web Surfing

Be suspicious of email requests, and call the sender to verify. Use safe web surfing practices. Consider a banking-only PC where email access and web surfing are not permitted.

## Dual Control

Implement enhanced online banking controls to authorize requested payments.

## Table-top Exercises

Implement and test your incident response plan often. Conduct exercises with key personnel to assess your readiness to respond to a cyber incident.

## Build Awareness

Enthusiastically promote cyber safety. Educate employees on the latest threats and reinforce company security policies.

# Resources

## CYBER RISK EXPOSURE SCORECARD

In recent years, cyber attacks have emerged as one of the most significant threats facing organizations of all sizes. The Internet and other network operations have created risks that were unheard of less than a decade ago. When cyber attacks (such as data breaches and hacks) occur, they can result in devastating damage, such as business disruptions, revenue loss, legal fees, and forensic analysis and customer or employee notifications.

It is important to remember that no organization is immune to the impact of cyber crime. As a result, cyber liability insurance has become an essential component to any risk management program.

**INSTRUCTIONS:** Begin by answering the questions below. Each response will be given a numerical value depending on the answer:

**YES:** 5 points  
**UNSURE:** 5 points  
**NO:** 0 points

After completing all of the questions, total your score to determine your organization's level of cyber risk using the scale below.

EXPOSURE	YES	NO	UNSURE	SCORE
1. Does your organization have a wireless network, or do employees or customers access your internal systems from remote locations?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
2. Does anyone in your organization take company-owned mobile devices (e.g., laptops, smartphones and USB drives) with them, either home or when travelling?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
3. Does your organization use Cloud-based software or storage?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
4. Does your organization have a "bring your own device" (BYOD) policy that allows employees to use personal devices for business use or on a company network?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
5. Are any employees allowed access to administrative privileges on your network or computers?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
6. Does your organization have critical operational systems connected to a public network?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
7. Does anyone in your organization use computers to access bank accounts or initiate money transfers?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
8. Does your organization store sensitive information (e.g., financial reports, trade secrets, intellectual property and product designs) that could potentially compromise your organization if stolen?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
9. Does your organization digitally store the personally identifiable information (PII) of employees or customers? This can include government-issued ID numbers and financial information.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
10. Is your organization part of a supply chain, or do you have supply chain partners?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
11. Does your organization conduct business in foreign countries, either physically or online?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
12. Has your organization ever failed to enforce policies around the acceptable use of computers, email, the Internet, etc.?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
13. Can the general public access your organization's building without the use of an ID card?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
14. Is network security training for employees optional at your organization?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
15. Can employees use their computers or company-issued devices indefinitely without updating passwords?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
16. Has your IT department ever failed to install antivirus software or perform regular vulnerability checks?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
17. Can employees dispose of sensitive information in unsecured bins?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
18. Would your organization lose critical information in the event of a system failure or other network disaster?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
19. Can employees easily see what co-workers are doing on their computers?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
20. Has your organization neglected to review its data security or cyber security policies and procedures within the last year?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
<b>TOTAL SCORE:</b>				

**ESCALATED RISK:** 55-100

**MODERATE RISK:** 15-25

**HIGH RISK:** 30-50

**LOW RISK:** 0-10

**NBT-MANG**  
INSURANCE  
AGENCY

© 2016 Zwire, Inc. All rights reserved.

# Common Themes

- Email & Web Surfing
- Dual Control
- Table-Tops
- And lastly...

# Build Cybersecurity Awareness

# Questions & Answers





Terra Carnrike-Granata  
Terra.Carnrike-Granata@nbtbci.com