

WIB/AABD Annual Directors Conference

Secrets of a Bank Hacker

**The latest scams and
solutions for your bank**

Presented by: Jim Sticklely

Why does security fail?

- You can have the best technology in the world yet be at great risk
- Through examples this session will help to explain why

Why target banks?

- Cash is not always the primary target
- Great source for information (ID Theft)
 - Name
 - Home Address
 - Social security number
 - Account numbers
 - Mothers maiden name
 - Loan information
 - Credit card information

How do hackers bypass security?

- Take advantage of common weaknesses
 - People don't understand the technology
 - People caught off guard
 - People trust other people
 - People trust the environment
 - People get careless

Security Risks Part 1

- People don't understand the technology

Confused about technology

- Online Viewer Exploits
 - With the rise of online video, flash programs and free games, new techniques are being deployed to trick people into loading malicious software

Online Viewer Exploits

- Starting the attack
 - Send email from Hallmark

To: jim@tracesecurity.com
Cc:
Subject: A Hallmark E-Card for you!



Shop Online

Hallmark Magazine

E-Cards & More

At Gold Crown

Someone Special has sent you a Hallmark E-Card.

Hello!

A Hallmark E-Card has been sent to you.

To see it, click [here](#),

or copy and paste the following link into your browser:

<http://www.hallmark-ecard.com/ECardWeb/ECV.jsp?a=429522245231>

There's something special about that E-Card feeling. We invite you to make a friend's day and [send one](#).

Hope to see you soon,
Your friends at Hallmark

Your privacy is our priority. Click the "Privacy and Security" link at the bottom of this E-mail to view our policy.



	Shop Online	Hallmark Magazine	E-Cards & More	At Gold Crown
--	-------------	-------------------	----------------	---------------

Search

You have an E-Card from Someone Special

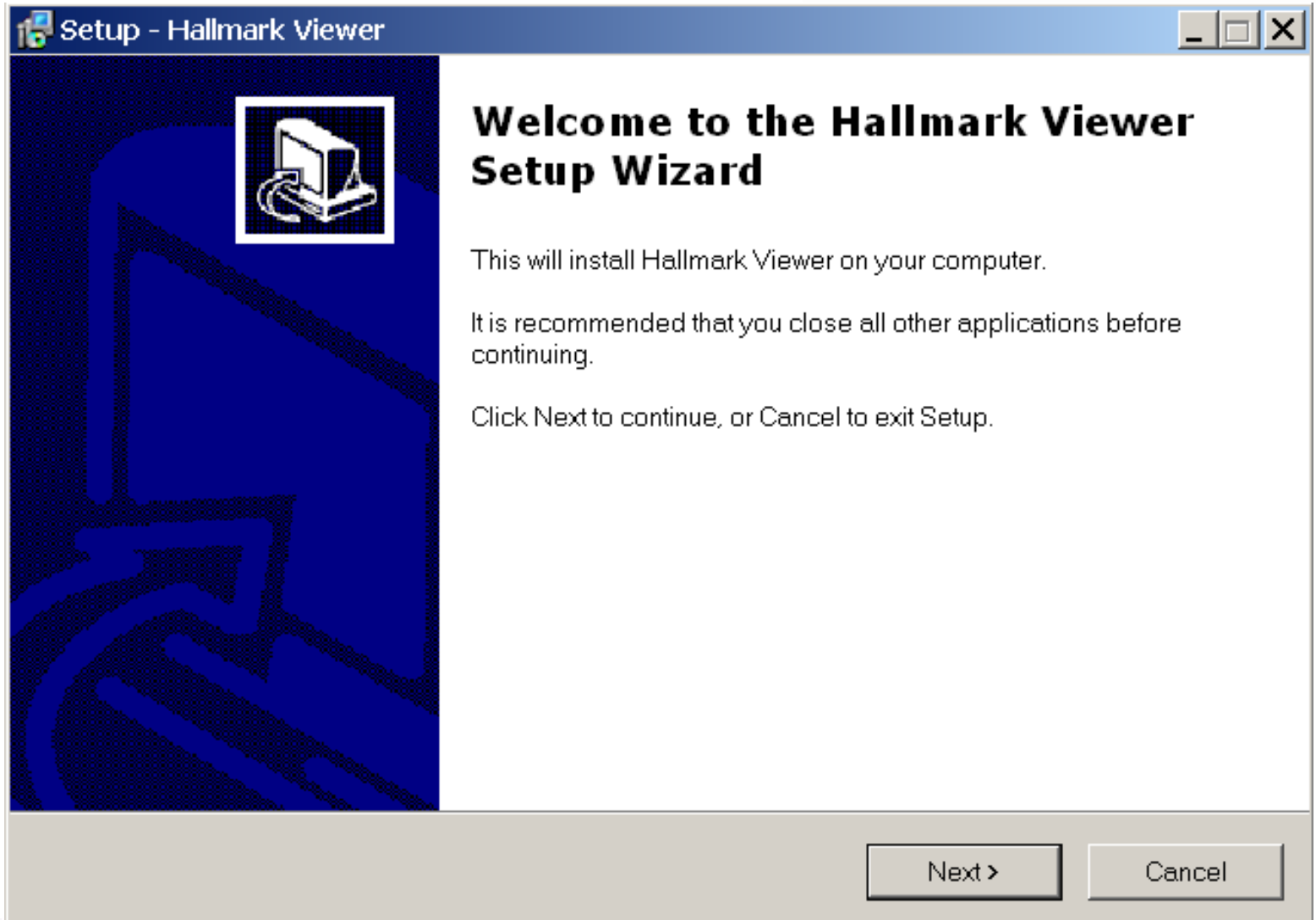
To use this product, you need to install free software

This product requires the Hallmark Video Viewer. To download this free software application, click the link below and follow the on-screen instructions.

Step 1: Download Hallmark Video Viewer
The Hallmark Video Viewer is free to download

Once the installations are complete, reload this page.






Hallmark.com: Products - Microsoft Internet Explorer

File Edit View Favorites Tools Help


← Back → Stop Home Search Favorites Media

Address http://192.168.1.1/ECardWeb/ECV.jsp?a=4295222452311M202018619Y&product_id=



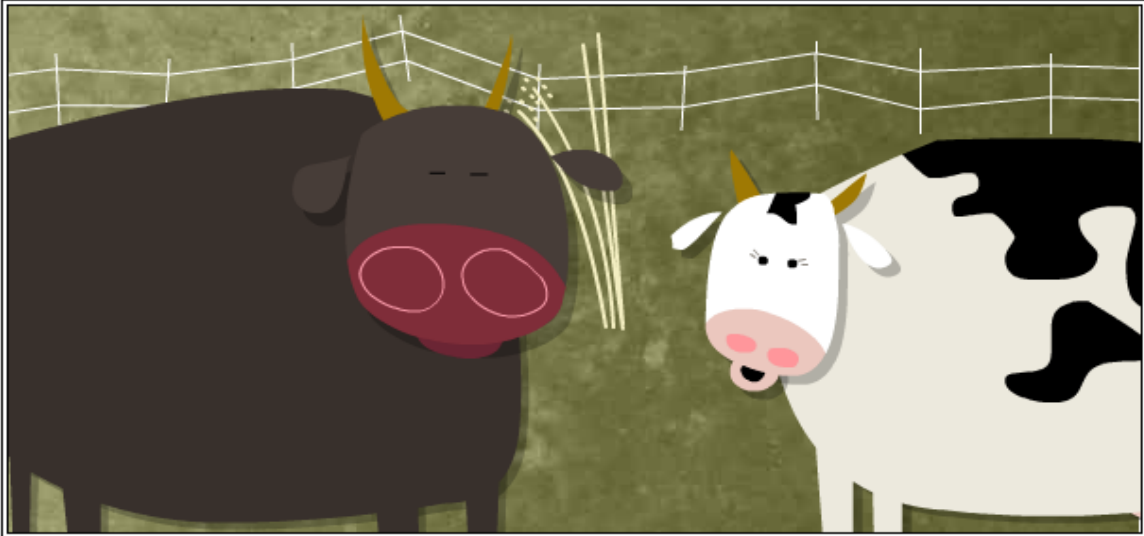
Hallmark .COM
Hallmark Quality, Online Convenience.

Make it fabulous...
Free Vase Upgrade
On Select Bouquets

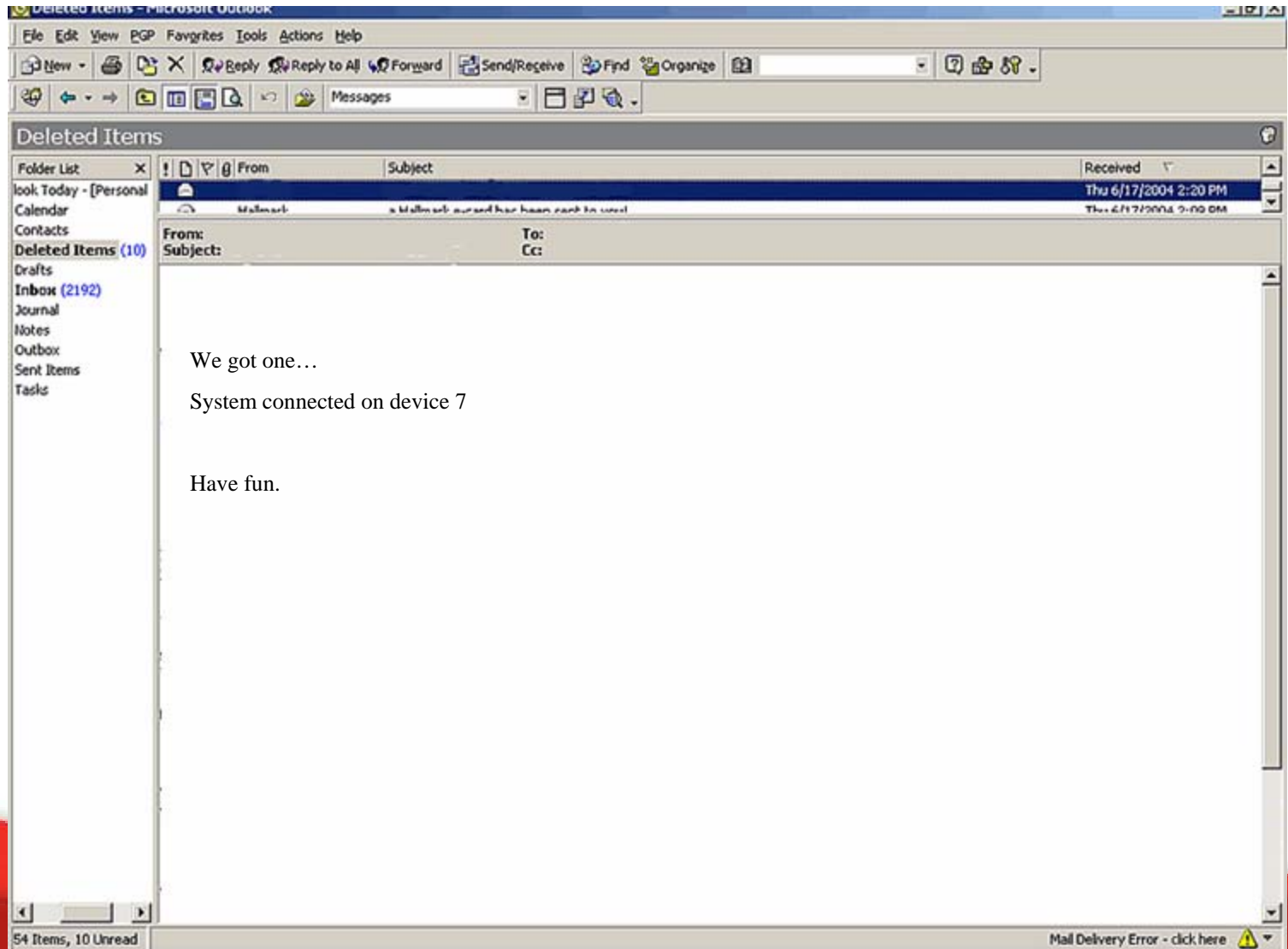
	Shop Online	Hallmark Magazine	E-Cards & More	At Gold Crown
---	-----------------------------	-----------------------------------	------------------------------------	-------------------------------

Sea

You have an E-Card from Someone Special



Online Viewer Exploits







Have a web cam?

This can be used to watch what you are doing without your knowledge

Online Viewer Exploit

- What is at risk?
 - Complete compromise of computer
 - Launch point for other attacks
 - Can “call home” at scheduled times
 - Bypass Firewall, Anti-Virus, IDS

Online Viewer Exploit

- Works for other sites as well...
 - YouTube
 - MySpace
 - NBC
 - ABC
 - FOX
 - Apple
 - Free Online games

Looking for YouTube Groups?

[Go to "Comr](#)

Banned Burger King Commercial - Safety Dance BK

To use this product, you need to install free software

This product requires the YouTube Video Viewer. To download this free software application, click the link below and follow the on-screen instructions.

Step 1: Download YouTube Video Viewer
The YouTube Video Viewer is free to download

Once the installations are complete, reload this page.



Added: **March 06, 2006**

SUBS

From: [RavenStake](#)

to Rave

COMEDIAN

Provided By:

[RavenStake](#)

<http://RavenStake.com>

Buy the T-Shirt!... ([more](#))

Category [Comedy](#)

Tags: [ravenstake](#) [burger](#) [king](#) [commercial](#)

URL <http://www.youtube.com/watch?v=oBbspkcoEgo>

Embed `<object width="425" height="350"><para`

Related

[More from this user](#)

Showing 1-20 of 30

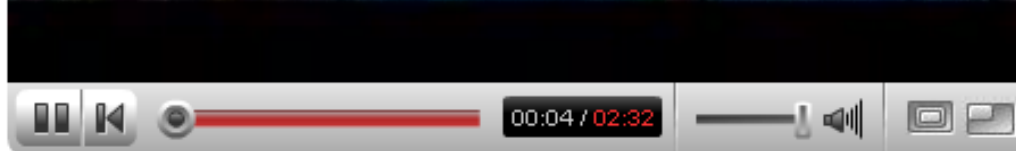
[See .](#)

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites Media Clock Print Mail RSS Feeds User

Address

Banned Burger King Commercial - Safety Dance BK



Added: **March 06, 2006**

From: [RavenStake](#)

Provided By: [COMEDIAN RavenStake](#)

<http://RavenStake.com>

Buy the T-Shirt!... ([more](#))

Category [Comedy](#)

Tags: [ravenstake](#) [burger](#) [king](#)

URL

Embed

[Related](#) [More from thi](#)

Showing 1–20 of 30

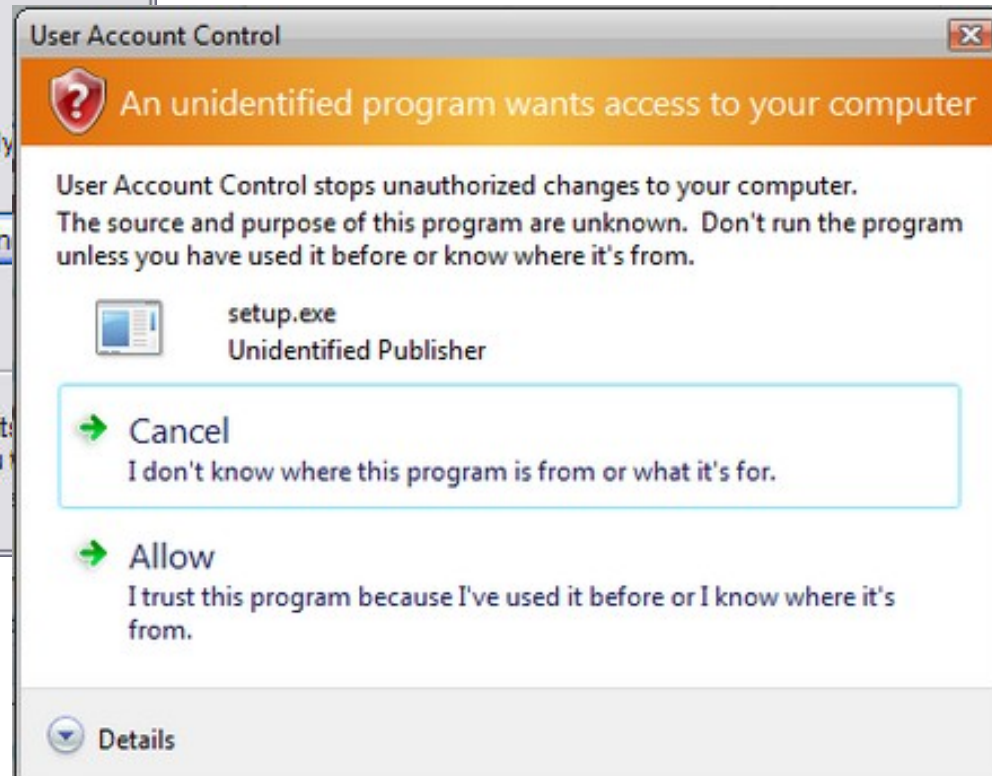
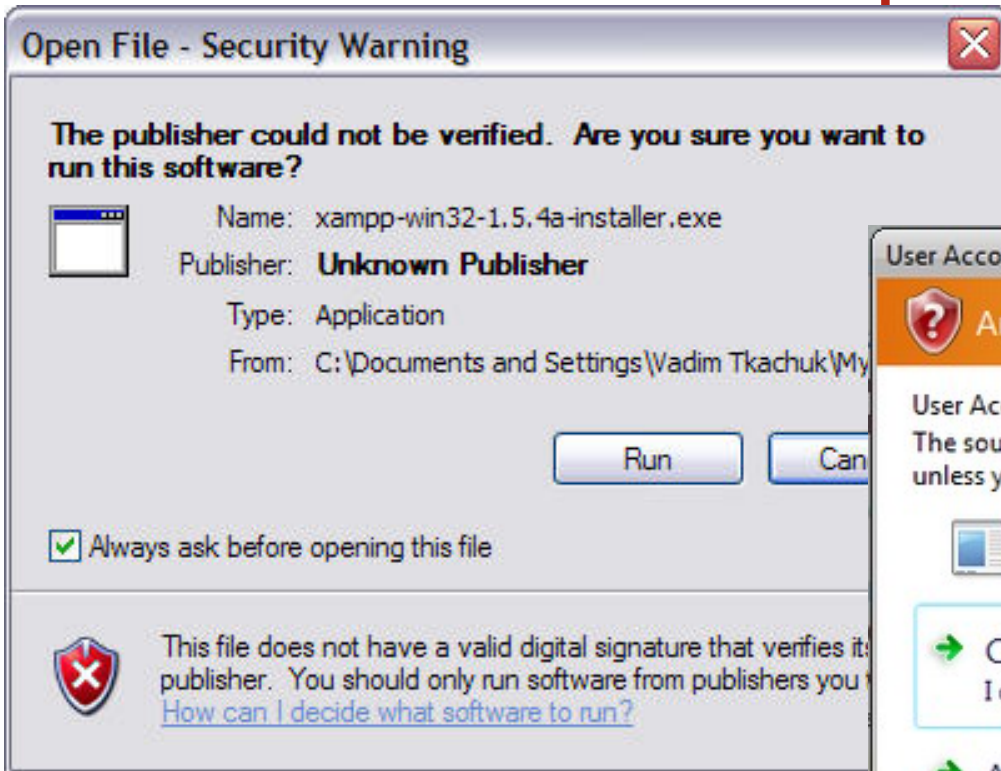


[Burger Kin
Snake Trij
Commerc](#)

Online Viewer Exploit

- What can you do to protect yourself?
 - Awareness Training
 - Pay attention to the site you are visiting
 - Verify the application has been digitally signed and trusted.

Online Viewer Exploit



Don't trust an application that has not been signed.

Security Risks Part 2

- People caught off guard

People caught off guard

- Vishing

- While most people have heard of “phishing” attacks, many are unaware of “Vishing”

Vishing

- What is Vishing?
 - Contacting people and requiring them to call back to an 800 number and convincing them to give confidential information using techniques that seem legitimate.
- Two main types
 - Direct Dial (Voicemail)
 - Shotgun Approach (Email)

Video →



Vishing

- What can be done?
 - Customer awareness
 - Let them know these types of attacks can happen
 - Don't send phone numbers in emails
 - Warn customers they should only call the number located on the back of their bank card.
 - Enforce strict shred policy
 - When in doubt, shred.
 - Recycle is not shred.
 - Center counter always missed.

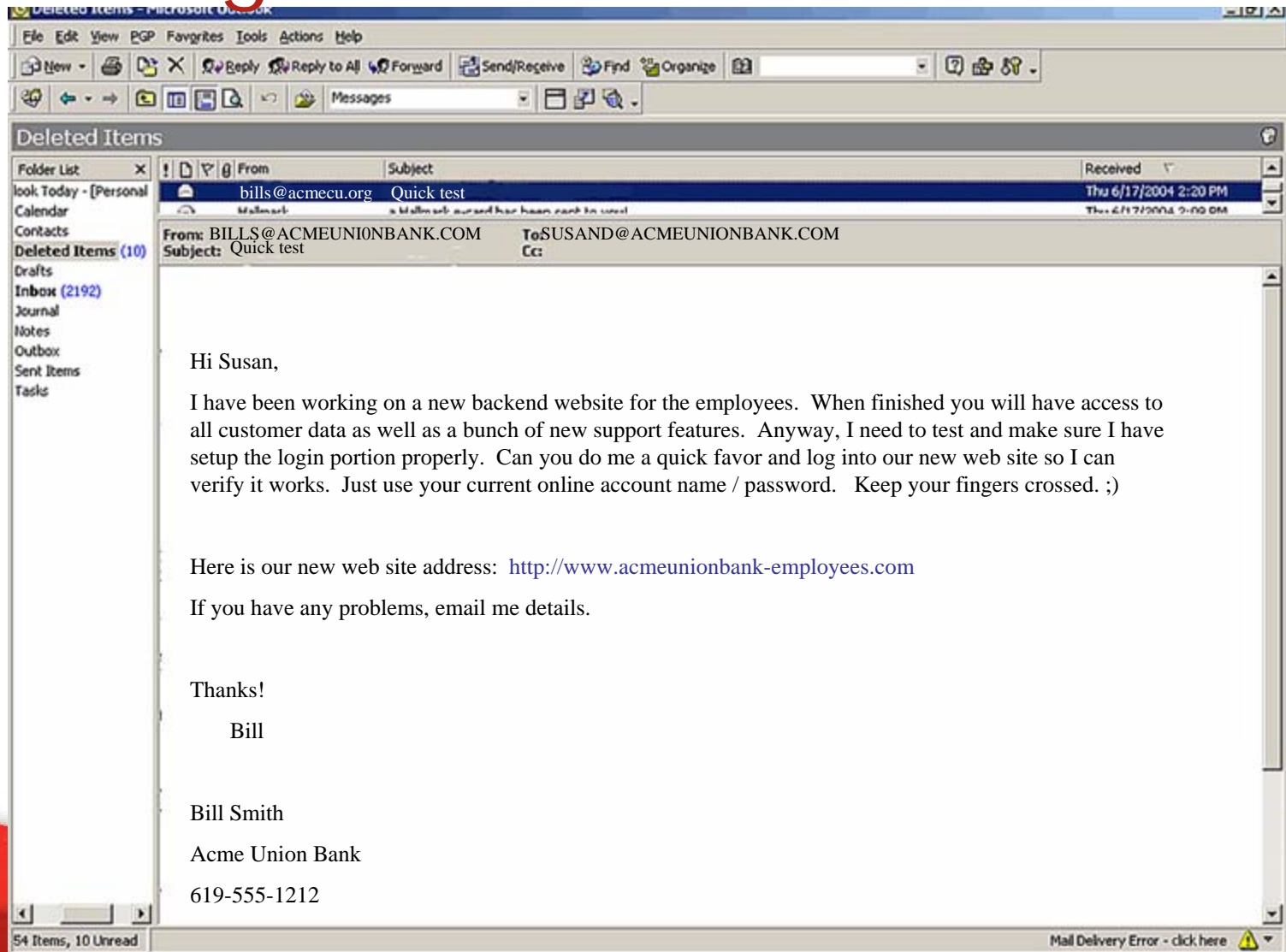
Security Risks Part 3

- People trust other people

Exploiting Co-workers

- Hijack a domain
 - Addresses use l in place of I or 0 in place of O
 - TRACESECURITY.COM
 - TRACESECURITY.COM
 - MODULARSECURITY.COM
 - MODULARSECURITY.COM

Exploiting Co-workers



Exploiting Co-workers

Employee Services Site


Home

Home | Documents | Policies | Training | Support | Calender | Tech Support | Help

Employee Services

Access ID:

Passcode:



Welcome to the Home Page

Please login for complete access.

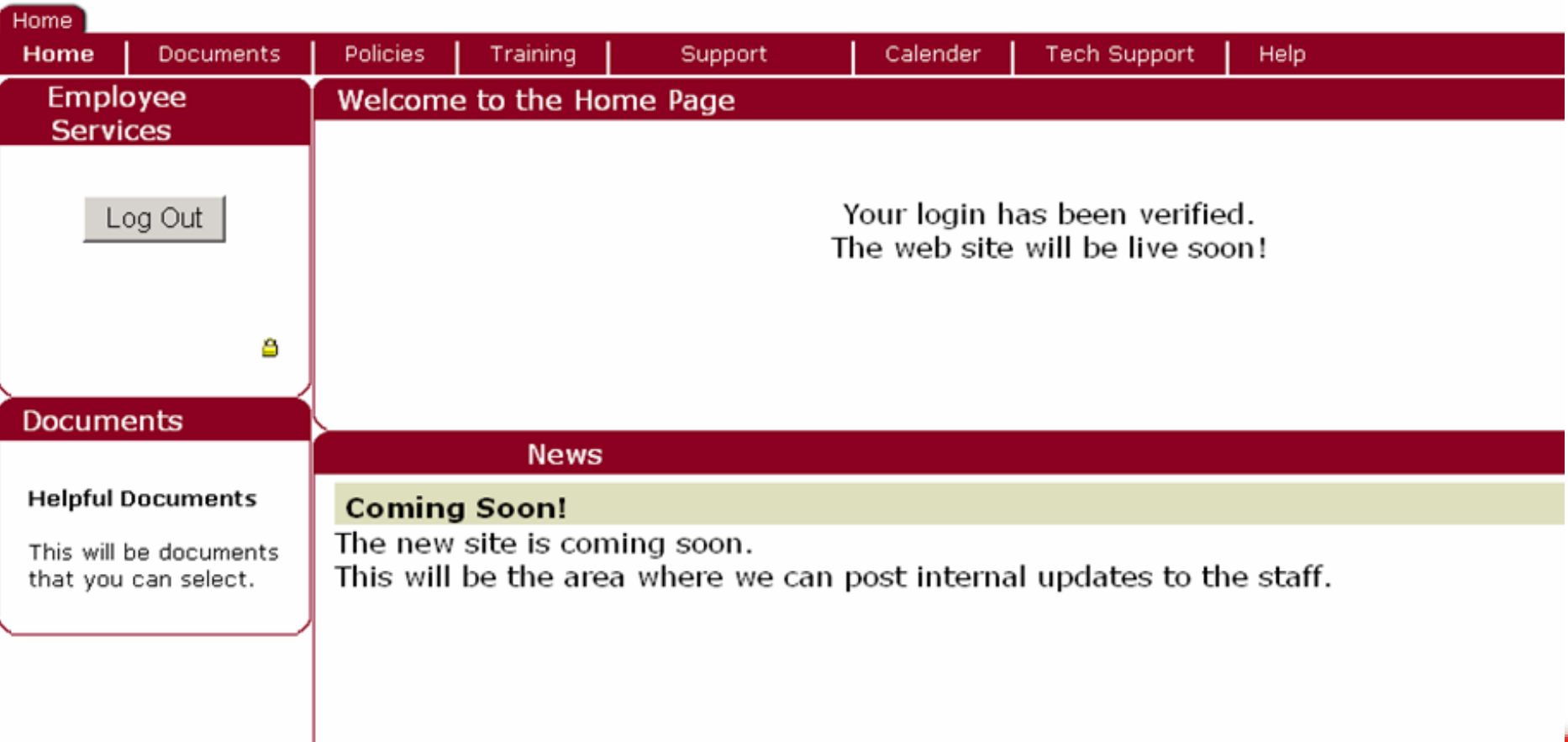
News

Coming Soon!
The new site is coming soon.
This will be the area where we can post internal updates to the staff.

Documents

Exploiting Co-workers

Employee Services Site



Home

Home | Documents | Policies | Training | Support | Calendar | Tech Support | Help

Employee Services

Log Out

Welcome to the Home Page

Your login has been verified.
The web site will be live soon!

Documents

Helpful Documents

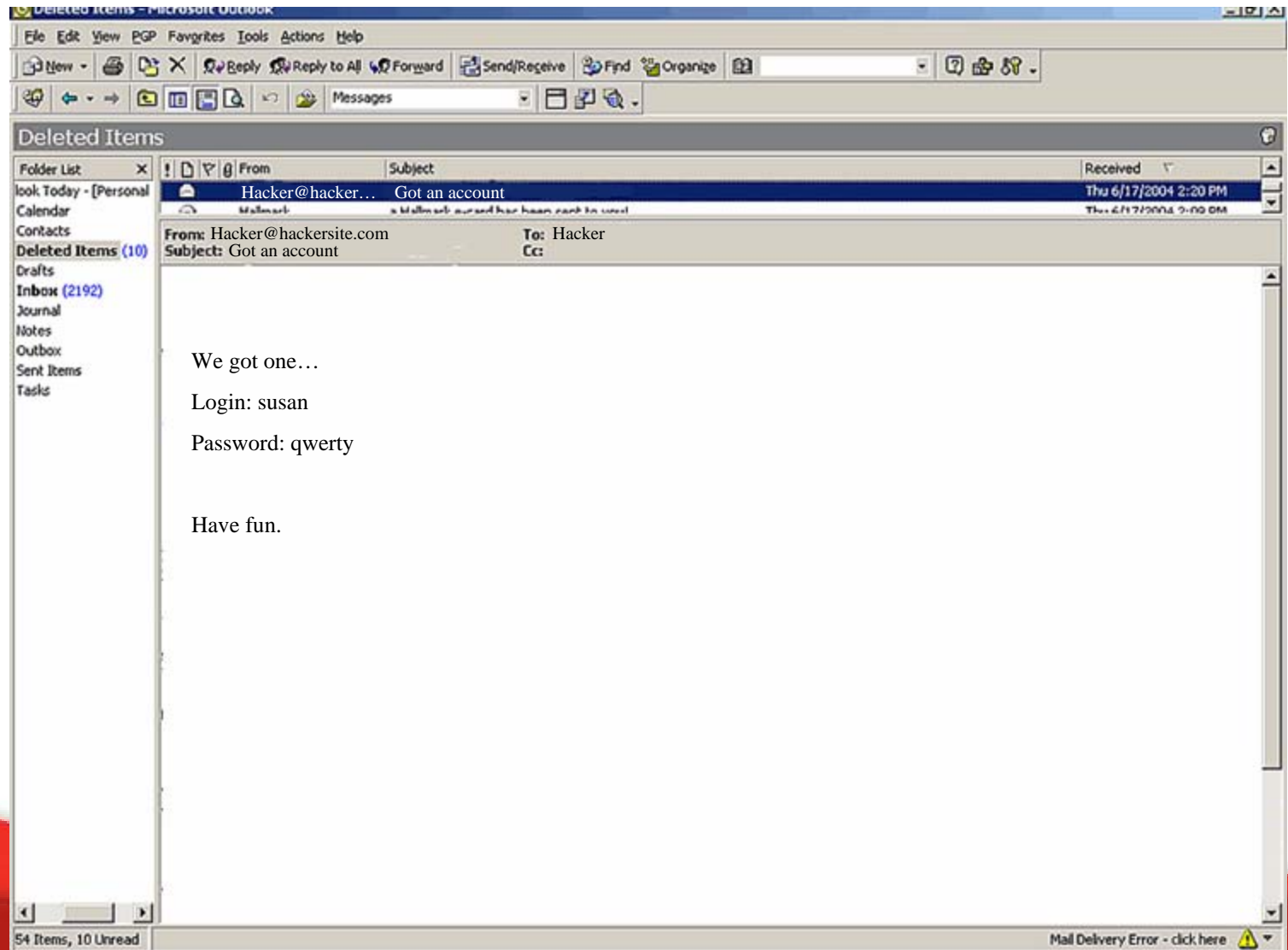
This will be documents that you can select.

News

Coming Soon!

The new site is coming soon.
This will be the area where we can post internal updates to the staff.

Exploiting Co-workers



Exploiting Co-workers

- How can this be prevented?
 - Employee awareness training
 - Don't trust emails
 - Never trust links in emails
 - Use the phone
- Be aware of other nasty side effects
 - Email contacts list often becomes corrupt

Exploiting Co-workers

- Other things you can do with trusted email
 - Convince employees to run trojaned software
 - Gain critical / confidential information
 - Request accounts to be created
- Run Trojans
- Gain confidential information

Security Risks Part 4

- People trust the environment
- 

People trust the environment

- Public computers major security risk
 - Hotels
 - Airports
 - Cyber Cafes
- Easy to compromise, difficult to detect
 - Keyboard loggers
 - Screen scrapers
 - Network Monitors

Video →



What can you do?

- Don't use public computers for secured transactions
- Change password frequently
- If you must use a public computer, copy and paste letters into text box

Security Risks Part 5

- People get careless

Inappropriate data on laptops

- Laptops have become the largest contributor to stolen confidential information
 - Bank of America
 - IRS
 - Department of Justice
 - UC Berkeley
 - Fidelity
 - Wells Fargo
 - San Jose Medical Group
 - Canadian Federal Government
 - George Bush Campaign Plans

Inappropriate data on laptops

- In 2005 750,000 laptops stolen
- Up from 600,000 in 2004
- 97% of all stolen laptops never recovered

Source: CNET

http://news.com.com/Getting+over+laptop+loss/2100-1044_3-6089921.html

Inappropriate data on laptops

- Do not store confidential information on laptops
- If something must be stored policy must dictate that it is encrypted
- Employee laptops used in the workplace is greatest risk

Policy and enforcement

- How do employees handle visitors?
 - Can visitors access secured areas unescorted?
 - Who is allowed on site?
 - Are they empowered to say no to requests from visitors?
 - What about employee communication between branches?

Lack of policy or enforcement

- How do employees handle visitors?
 - Social engineering, easier then it sounds.

Video →



Policy and enforcement

- What can be done?
 - Identification must be verified when accessing secured areas
 - Policy must state visitors to be escorted at all times in secured areas
 - Confidential papers should not be in areas where public has access
 - Open communication channel between branches

Become Proactive

- Simply responding to security threats is not enough

Get the word out

- Warn customers through monthly statements
 - Both Online and Paper
- Warn customers through news letters
- Offer Security training seminars for your customers
- Continue to educate your employees

In the end...

- You can't prevent every security risk
- You can educate others to be suspicious
- Remember that you can spend hundreds of thousands on security products and it just takes one human mistake to bypass it all

TraceSecurity Inc.

Comprehensive Security & Risk Assessments

IT Audits

Penetration Testing

Comprehensive Regulation Compliance Review

Online Banking Application Testing

Remote and Onsite Social Engineering

Policy Development and Review

Numerous Training Courses available (On site and remote)

Anti Phishing, Man in the Middle and Pharming solution

Multi Factor Authentication Solution