



---

---

---

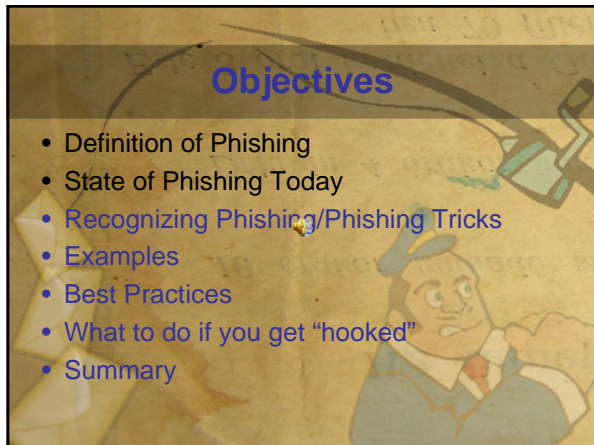
---

---

---

---

---



---

---

---

---

---

---

---

---



---

---

---

---

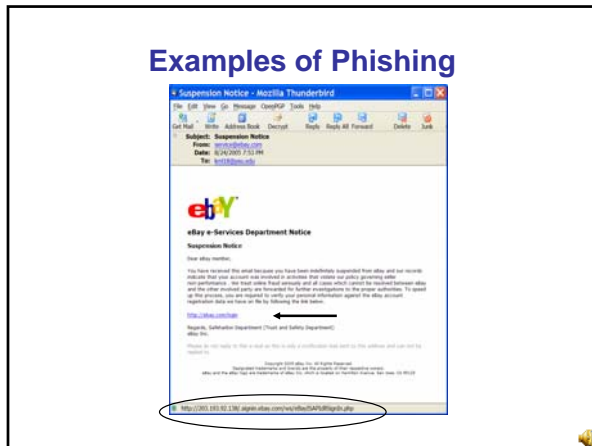
---

---

---

---

## Examples of Phishing




---

---

---

---

---

---

---

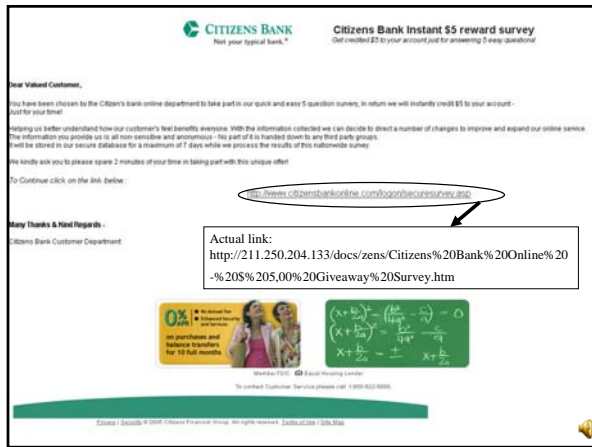
---

---

---

---

---




---

---

---

---

---

---

---

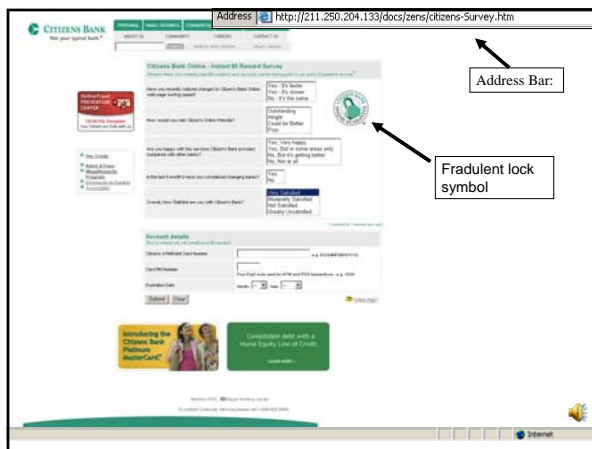
---

---

---

---

---




---

---

---

---

---

---

---

---

---

---

---

---

## Looks persuasive...

X-Sense-UUID: 06270933-0E11-4119-B93A-CED9849999E2  
X-Sense-UUID: EC567E04-4760-4F66-903F-038000016500  
From: "LaSalleBank" <important@lasallebank.com>  
Subject: IMPORTANT: Account Verification  
Date: Wed, 22 Jun 2005 03:50:16 -0700  
X-Mailer: Microsoft Outlook Express 6.00.2600.0000  
To: undelivered\_recipients...  
X-WSS-ID: 6E4687CC29F77526-01-04  
X-OriginalArrivalTime: 22 Jun 2005 00:53:26.0127 (UTC)  
FILETIME=[CC2FA7F0-01C576C4]  
X-WSS-ID: 6E4687AF253180796-01-04



We are glad to inform you, that our bank has a new security system. The new updated technology will ensure the security of your payments through our bank.

Hoping you understand that we are doing this for your own safety we suggest you to update your account. This update will maintain the safety of your account. All you have to do is to complete our online secured form. Thank You.

[Continue](#)

---

---

---

---

---

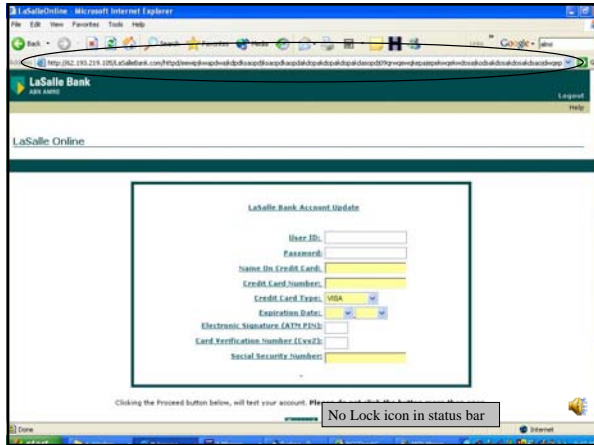
---

---

---

---

---



No Lock icon in status bar

---

---

---

---

---

---

---

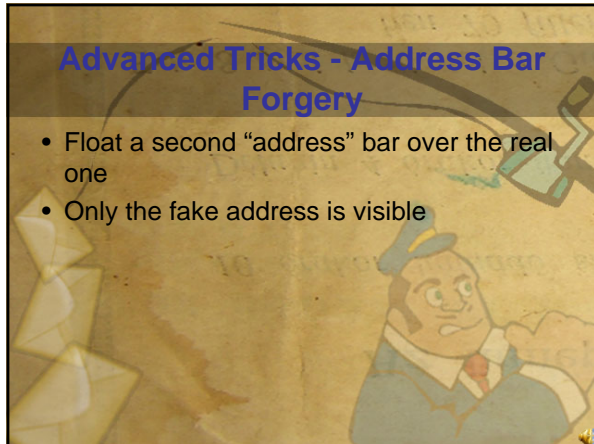
---

---

---

## Advanced Tricks - Address Bar Forgery

- Float a second "address" bar over the real one
- Only the fake address is visible



---

---

---

---

---

---

---

---

---

---



## Forged Address Bar and Forged ToolTip



Dear Huntington Bank customer,

Technical services of the Bank are carrying out a planned software upgrade for the maximum convenience of the users of e-services of the Huntington Bank. We earnestly ask you to visit the following link and to confirm your bank data.

To securely confirm your Huntington Bank details please go to:

<https://onlinebanking.huntington.com/egx.asp?confirm=yes>

This instruction has been sent to [John.Cusumano@huntington.com](mailto:John.Cusumano@huntington.com)

We present our apologies and thank you for co-operating

The forged tooltip

---

---

---

---

---

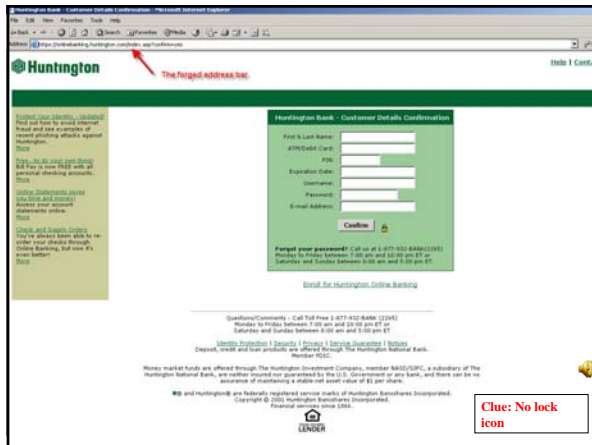
---

---

---

---

---



---

---

---

---

---

---

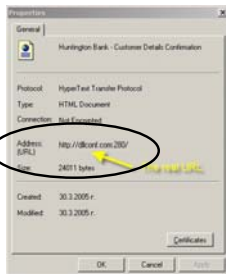
---

---

---

---

## File-Properties displays the real web address:



---

---

---

---

---

---

---

---

---

---

**Best Practices: What You Can Do**

- Be suspicious by default
- Scrutinize web addresses: verify link targets
- Don't visit sites via links – use bookmarks and keywords or type in the web address
- Disclose email address only when necessary
- Check to make sure the Web site is using encryption (secure site **https**)
  - Lock icon appears in the lower right-hand corner of the status bar

---

---

---

---

---

---

---

---

**Best Practices: What You Can Do**

- Don't be put at ease by language that suggests a concern for your security
- Know common formats of fraudulent links
- Never respond to requests for personal information via e-mail or in a pop-up window
- You can forward phishing messages to [spam@uce.gov](mailto:spam@uce.gov)

---

---

---

---

---

---

---

---

**Best Practices: Know what to look for**

- Impersonal or generic greetings
- Time limited offers or urgent requests for personal information
- Fake links
- Spelling mistakes and poor grammar
- Attachments – DON'T open them
- NEVER log into any account from a link in an email

---

---

---

---

---

---

---

---

**What to do if you get “hooked”**

- Alert the Credit Bureaus
  - Will put an ‘alert’ on your file for 90 days
- Request a copy of your credit report
  - [www.annualcreditreport.com](http://www.annualcreditreport.com)
  - Entitled to one free report per year
- Require written notice to extend credit

---

---

---

---

---

---

---

---

**What to do if you get “hooked”**

- Inform the impersonated company or person
- Close the account, reopen new one
- Report fraud to [www.fraud.org](http://www.fraud.org)
- Notify the credit bureaus
- Optionally, file a police report
  - Can be useful if evidence is needed for creditors

---

---

---

---

---

---

---

---

**What to do if you get “hooked”**

- File a complaint with the FTC
  - File a complaint at <http://ftc.gov/> or call the FTC at 1-800-FTC-HELP (1-877-382-4357)
  - Helps to coordinate efforts to combat fraud

---

---

---

---

---

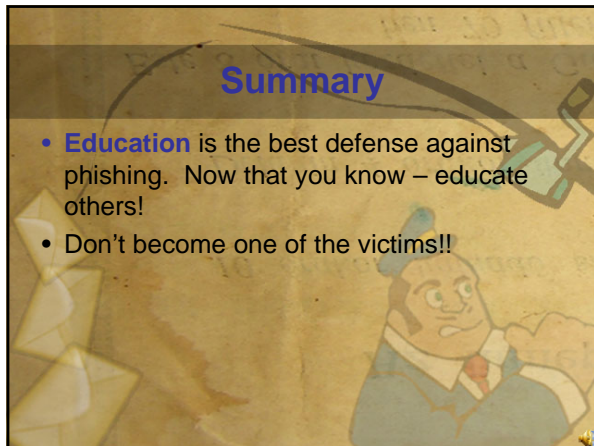
---

---

---

## Summary

- **Education** is the best defense against phishing. Now that you know – educate others!
- Don't become one of the victims!!



---

---

---

---

---

---

---

---

## Resources

- Office of General Counsel Identify Theft:
  - <http://www.uakron.edu/ogc/PreventiveLaw/identitytheft.php>
- Anti-Phishing Working Group:
  - <http://www.antiphishing.org/index.html>
- Identity theft website:
  - <http://www.consumer.gov/idtheft/>
- Consumer Fraud Reporting:
  - [www.consumerfraudreporting.org](http://www.consumerfraudreporting.org)
- Internet and Telemarketing Fraud:
  - <http://www.fraud.org/>



---

---

---

---

---

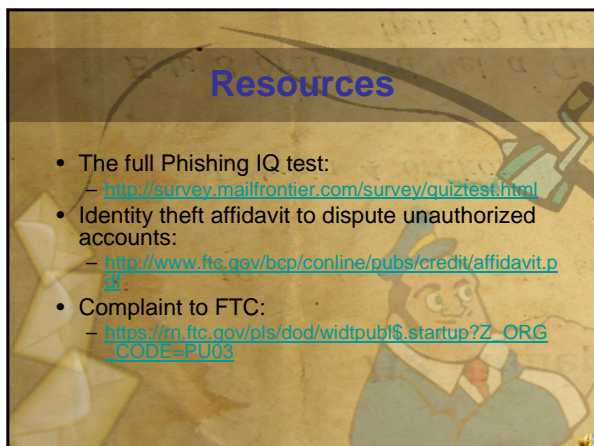
---

---

---

## Resources

- The full Phishing IQ test:
  - <http://survey.mailfrontier.com/survey/quiztest.html>
- Identity theft affidavit to dispute unauthorized accounts:
  - [http://www.ftc.gov/bcp/online/pubs/credit/affidavit.p](http://www.ftc.gov/bcp/online/pubs/credit/affidavit.pdf)
- Complaint to FTC:
  - [https://n.ftc.gov/pls/dod/widtpub\\$.startup?Z\\_ORG\\_CODE=PU03](https://n.ftc.gov/pls/dod/widtpub$.startup?Z_ORG_CODE=PU03)



---

---

---

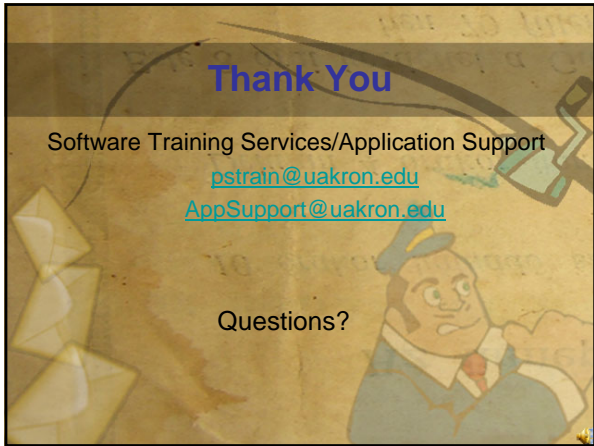
---

---

---

---

---



---

---

---

---

---

---

---

---