# The Threat of Phishing and Financial Spyware Scams

Toby Kohlenberg and Lenny Zeltser

SANS Internet Storm Center

August 4, 2004

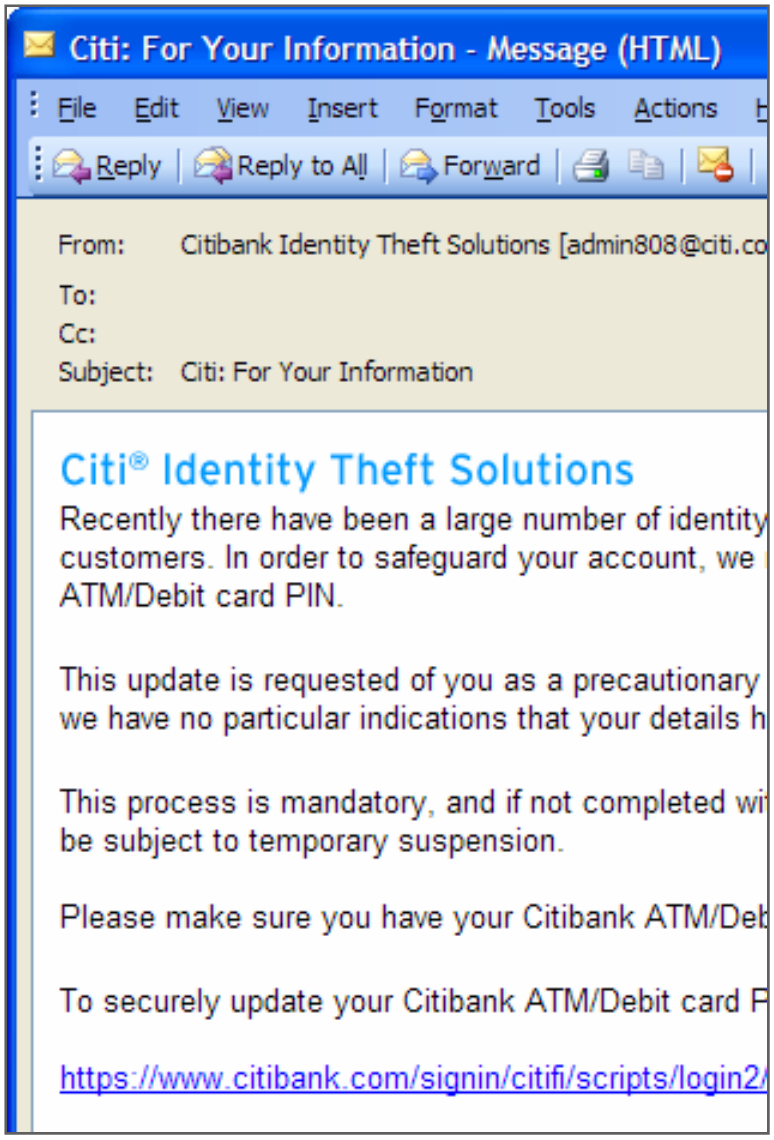
# Consumer financial information is increasingly targeted on the Internet

- Many attack schemes
- Phishing scams
- Financial spyware

We will look at these threats

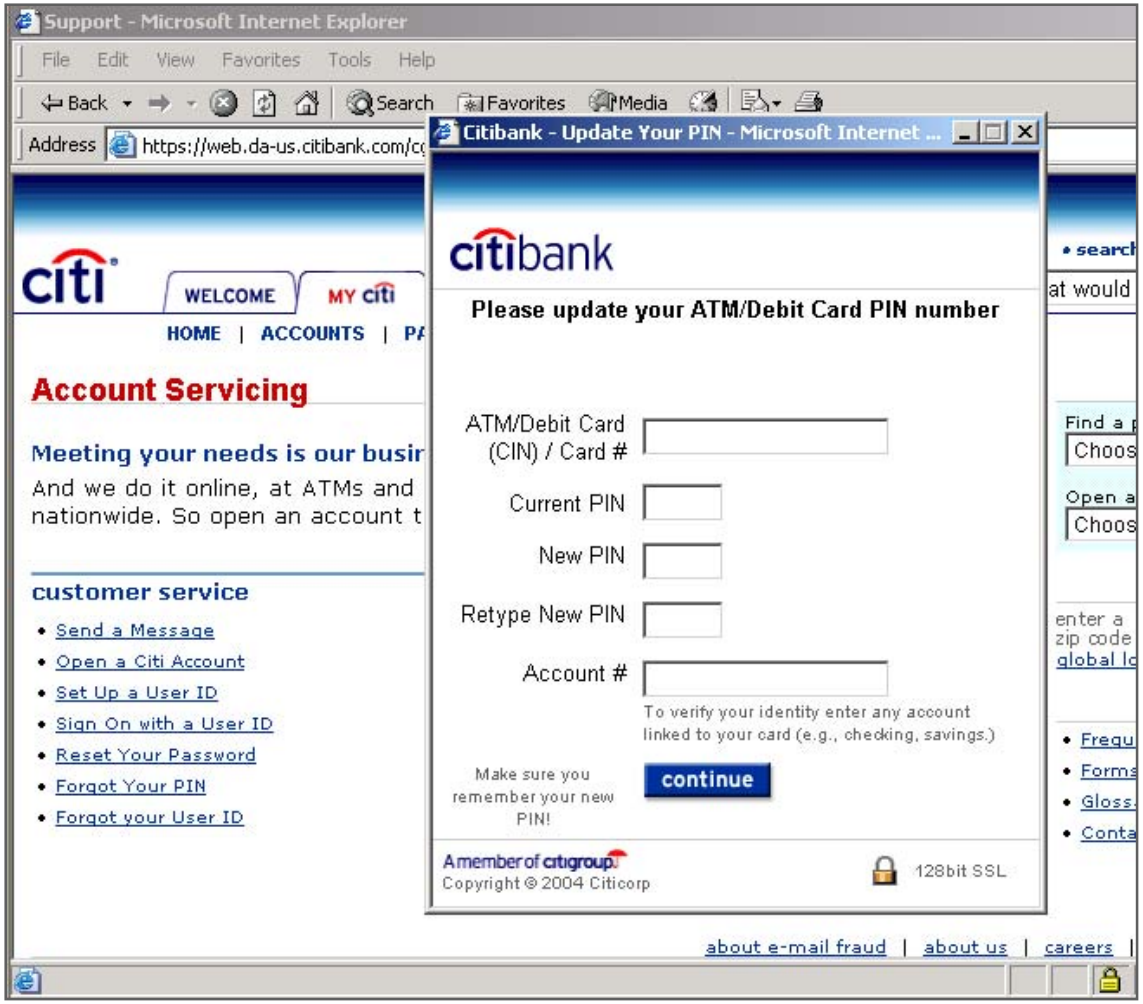
# 28% of consumers are fooled by phishing scams

- Messages crafted to look legitimate
- The link goes to a fraudulent website
- 41% of U.S. adults have, or think they have, received a phishing email



# It can be very hard to visually detect a fraudulent financial website

- Real Citibank site opens on background
- Fraudulent window pops up on top
- Seems secure and authentic (note the lock)



# Financial spyware is another way of stealing personal information

- Consumers may get infected when visiting malicious websites
- Malicious program monitors the victim's financial activity
- Spyware may also spread via e-mail or come bundled with legitimate software

# A recent spyware attacked using a pop-up ad and then captured financial data

Attack:

- Exploited a flaw in Internet Explorer

Result:

- Spyware captured financial information
- Stole data despite browser encryption

# Another spyware combined phishing and keystroke-recording attacks

- Exploited a flaw in Internet Explorer
- Consumers infected via malicious websites
- Captured passwords when victims logged into eBay, PayPal, etc.
- Created a fake pop-up window that asked for credit card information

# Spyware is a significant threat to consumers' financial information

- Can bypass encryption mechanisms
- Takes advantage of software flaws
- Anti-virus software not always effective
- Victims usually unaware of being spied on
- Out of 1.5 million PCs scanned, 500,000 instances of spyware was found

# Several ways of addressing phishing and financial spyware threats

- Consumer awareness campaign
- Addressing software vulnerabilities
- Faster financial smart-card adoption
- Clear disclosure of software actions
- Enforcement of privacy breach disclosure