



Cyber Crimes and Workplace Security


Susan Wind
Wind & Hazen Associates Inc.
www.windandhazen.com
Susan@windandhazen.com



#1 Priority



Safety



Security

Overview

- Cybercrime and Security
- Crimes that affect the workplace
- Prevention Methods

What is Cybercrime?

According to the Department of Justice, a cybercrime is “any violations of criminal law that involve knowledge of computer technology for their perception, investigation, or prosecution”.

AKA: Crimes on the Internet



Types of Cyber Attacks

- Adware, Spyware, Malware, Spam
- Phishing
- Botnets

Adware

- Bundled with many software packages/downloads
- Free software that is supported by advertisements
- Most adware is safe, however some can serve as spyware (which gathers information from your computer)
- Look for the 3rd party clause!

Spyware

- Computer software/application that gathers and reports information about a computer user without their knowledge or consent.



Malware

- Malicious computer software that interferes with normal computer functions or sends personal data about the user to unauthorized parties over the Internet.
- Goal – corrupt a computer/obtain data illegally
- Email attachments (worms, viruses, trojan horse)

Phishing

- A computer scam where the perpetrator tries to get sensitive information by sending users to fake, but legitimate looking websites.
- The most common scam people fall victim to
- The goal – to steal your identity



Phishing (cont)

- They may appear from a financial institution or a company you conduct business with
- They appear to be from someone you know (employer, colleague, human resource department)
- They ask you to call a phone #
- They include official looking logos taken directly from their websites
- They include links to “spoofed” websites

Phishing (cont)

- The website is deceptive
- Common phrases are:
 - Verify Account information
 - You have won
 - If you don't respond within 24 hours, your account will be suspended
 - Click the link below to gain access to your account
 - Click the link below to unsubscribe to this email

Phishing Examples

- Spoofed websites will look very similar to original
 - www.business.com
 - www.busness.com
 - www.verifybusiness.com
 - www.businesss.com

Phishing Examples

- Ebay
- Clearinghouse
- Financial Institutions (banks, credit unions)
- Craigs List
- Paypal



Botnets

Also called a "zombie army," a botnet is a large number of compromised computers that are used to create and send spam or viruses or flood a network with messages as a denial of service attack. The computer is compromised via a Trojan that often works by opening an Internet Relay Chat (IRC) channel that waits for commands from the person in control of the botnet. There is a thriving botnet business selling lists of compromised computers to hackers and spammers.

(YourDictionary.com)

Prevention Tactics

- Security Measures
- Accountability
- Education

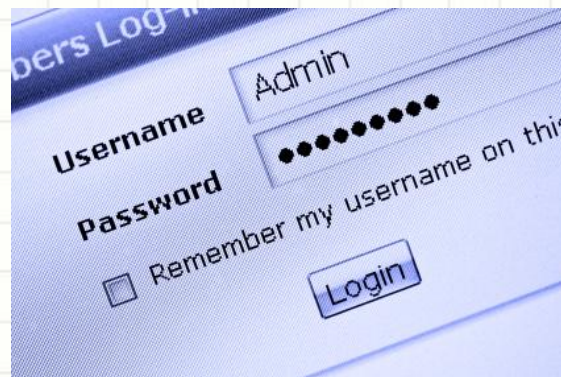


Security Measures

- Information Security
 - Secure all software/hardware
 - Strong passwords
 - Monitor and validate controls
 - Updated anti-virus software applications
 - Firewalls
 - Block websites
 - Utilize outside vendors to monitor computer usage

Accountability

- Policies in place (internet vs intranet)
- Monitor internet usage



Education

- Attend trainings
- Newsletters
- Round table exercises
- Network



Crimes within the workplace

What all employers should know!



Types of Threats

- Internal
- External

Internal Threats (online)

- Theft
- Harassment

© Original Artist
Reproduction rights obtainable from
www.CartoonStock.com



Thefts

- Identity Theft/Fraud



Common trends

- Dumpster Diving
- Accessible Computers
- Frequent unauthorized areas
- Mysterious Disappearances



Motive and “signs”

- Changes in behavior
- Feeling of urgency
- Confident that he/she will not be caught

- Economy
- Drugs
- Change in lifestyle

Harassment

- Taking place through Social Network websites, emails, text messages
 - Bitter employees
 - Sexual
 - Relationship



External Threats (online)

- Theft
- Fraud



Theft/Fraud

- Identity theft
- Hackers
- Scams



Recent scams

- Canadian Lottery Scam
- Work from home scams
- Secret Shoppers
- Phishing



Examples

- **INTERNATIONAL MONETARY FUND (IMF)
DEPT: WORLD DEBT RECONCILIATION AGENCIES.
ADVISE: YOUR OUTSTANDING PAYMENT NOTIFICATION**

Attn: Fund Owner,

Your Long overdue Payment.

Your email was found (in the Central Computer among the list of unpaid contractors, inheritance next of kin and lotto beneficiaries that was originated from Africa, Europe, Asia Plus Middle east, Americans) among the list of individuals and companies that your unpaid fund has been located to the CITI BANK OF LONDON. Your email appeared among the beneficiaries, who will receive a part-payment of your contractual sum of (11 million United State Dollars) and it have been approved already for months.

However, we received an email from one Mr. Virgle Lee Samples who told us that he is your next of kin and that you died in a car accident last week. He has also submitted his account for us to transfer the fund to him including his International passport; we want to hear from you before we can make the transfer to confirm if you are dead or not? Please if you are still alive, kindly furnish us with below information:

Examples

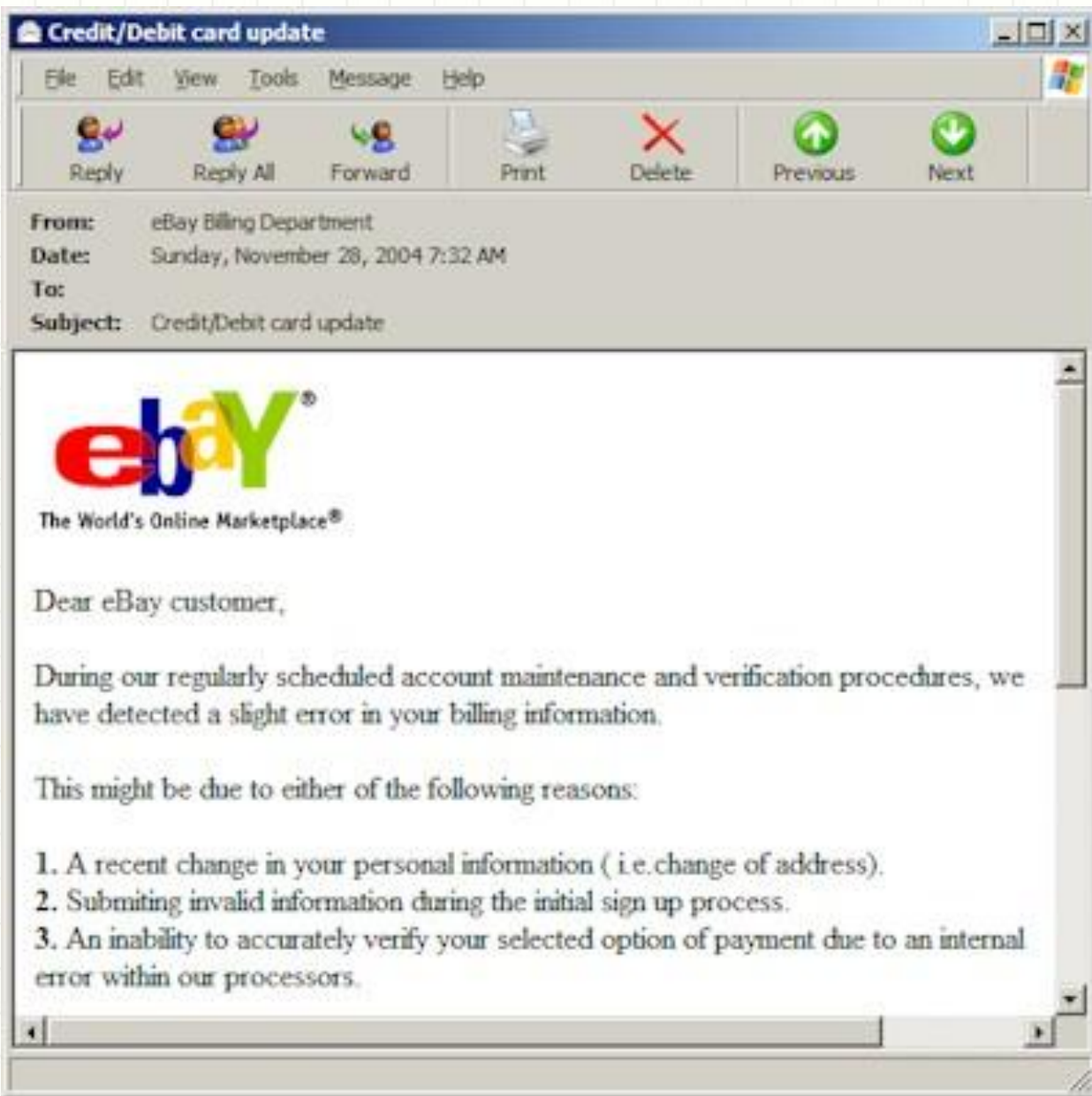
- **1. Your Full Name.....**
2. Address.....
3. Country.....
4. Age.....
5. Occupation.....
6. Telephone Number.....
7. Next Of Kin.....
8. Home Equity (Yes/No).....

Once again, I apologize to you on behalf Of IMF (International Monetary Fund) for failure to pay your funds in time, which according to records in the system had been long overdue. I wait to hear from you soonest.

Your quick response will be highly appreciated.

Regards,

**Mr.Mark Peterson.
Office of the IMF London,
United Kingdom.
EMAIL:unpaidfund2009@live.co.uk**



Social Network Websites

- Facebook
- Twitter
- Myspace
- Formspring

Issues behind them!

- Legal concerns – Freedom of Speech and Search and Seizure
- Liability
- Bullying
- Exploitation
- Harassment

Prevention Methods

Where do you start?

- Assessing the risks
- Assessing the vulnerabilities

PREVENTION IS DONE THROUGH

AWARENESS



TRAINING



ACCOUNTABILITY

Internal Threats

- How well do you know your employees?
- Training
- Thorough background investigations
- Audits
- Frequent evaluations

External Threats

- Security equipment – up to date technology
- CPTED – Crime Prevention Through Environmental Design
- Network with police
- Involvement with community
- Crime Statistics

Philosophy of CPTED

- Strategies used to influence decisions that precede criminal behavior
- Creating psychological barriers through physical means to prevent crime
- Methods that emphasize enhancing the perceived risk of detection and apprehension

CPTED Examples


- Parking lots
- Lobbies
- Lighting
- Landscape
- Location
- Cameras
- Greeters



Education is key!

- Quarterly training
- In – House
- Seminars
- Webinars
- Newsletters
- Website





What do you have to lose?



QUESTIONS?



Thank you!

**For additional information, please contact me at
susan@windandhazen.com**