

Cybercrime

Don't be a Victim



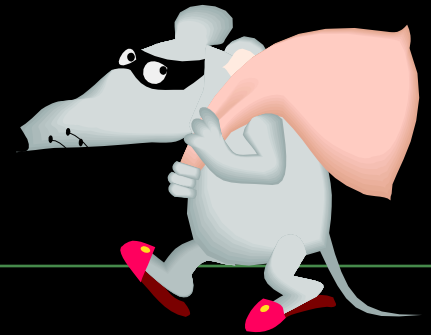
**Presenter:
Teron Greenidge**



Objectives

- To provide a general awareness of Cybercrime
- To Recognize Cybercrime methods
- To identify Internet scams
- To learn how to keep from being a victim

What is Cybercrime?



- Cybercrime – also known as computer crime, e-crime and electronic crime is a criminal act where a computer or computer network serves as the location, means, target or as the source of the activity.
 - Types range from outside parties who hack into a computer network to phishing programs which give users a false sense of security, prompting them to divulge sensitive information.

Effects of Cybercrime

- Lost of Revenue

- This lost can be caused by an outside party who obtains sensitive financial information, using it to withdraw funds from an organisation.
 - Drive by hackers

- Wasted Time

Effects of Cybercrime

■ Damaged Reputations

- In cases where computer records are compromised by a security breach associated with Cybercrime.
- Credit Cards or other Financial Data become intercepted.

■ Reduced Productivity

- Due to the measures that many companies must implement to counteract Cybercrime, there is often a negative effect on employees productivity.

Simple Theory

- When you purchase a home it comes with a door and a lock. You always ensure that the door/lock exist and working properly. You may even purchase security systems.
- Well, why would you not secure your investments?

Tools of the Trade

- Wireless networking technology poses the biggest problem, as an unsecured network can be hacked into anywhere outside using a simple radio antenna, PDA or Cell phone
- Password crackers

Tools of the Trade

- Network Scanning software that looks for open ports to gain access to the network
- Illegitimate websites, to lure you into giving information over the web
- Spam

Examples of Cybercrime

- Hacking/ cracking
- Cyber-Stalking
- Internet fraud
- Phishing
- Electronic Money Laundering
- Identity theft
- Salami attack
- Interception and fabrication of emails
- Theft of passwords
- Computer Viruses

Who are the perpetrators?

- Not just “hackers.”
 - Companies seeking competitor’s trade secrets
 - Con-artists
 - Pedophiles
 - Disgruntled employees
 - “Accidental” criminals
- The Internet should be viewed as another medium in which criminals can conduct illegal acts.



Who are the cyber victims?

- Companies

- No security awareness
- Bottom liners

- Individuals

- The unaware individuals
- The “don’t care” individuals
- The “innocent by-stander” individuals

- Society

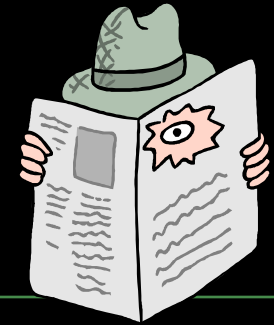


Desktop Security



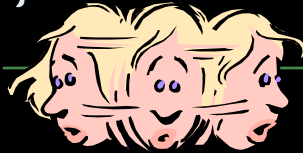
- Many people become victims of a cyber attack by what is referred to as “drive by hacking.”
- Tools are freely available on the Internet to allow for such behavior to occur.
- The latest Microsoft Security flaw is a good example of how vulnerable each users desktop is to such an attack.

Spyware



- Spyware is used by companies to gather the surfing habits of individuals.
- Pop-up ads are usually a result of spyware being present on a computer.
- Keyloggers are a form of spyware that secretly record keystrokes and have the ability to email them back to the intruder.

What can I do?



- Awareness is the first step in protecting yourself, your family and your business.
- Invest in Anti-virus, Firewall, and SPAM blocking software for your PC.
- Detect secure websites when conducting transactions online.
- Do NOT respond or act on emails sent from unknown sources.

Detecting Secure Websites

The screenshot shows a Microsoft Internet Explorer browser window displaying the Outlook Web Access login page. The address bar shows the URL: `https://woa.stcc.cc.tx.us/exchange/logon.asp`. The page content includes the Outlook Web Access logo, a description of the service, and login options for Exchange Users and Public Access. A red arrow points to the URL in the address bar, and another red arrow points to the yellow lock icon in the status bar at the bottom right of the browser window.

Microsoft Outlook Web Access
for Microsoft (R) Exchange Server

Version 5.5 SP4

Microsoft (R) Outlook (TM) Web Access is a Microsoft Exchange Active Server Application that gives you private access to your Microsoft Outlook or Microsoft Exchange personal e-mail account so that you can view your Inbox from any Web Browser. It also allows you to view Exchange server public folders and the Address Book from the World Wide Web. Anyone can post messages anonymously to public folders or search for users in the Address Book. For more information about this Outlook product, [click here](#).

Log On

Exchange Users Only:
Type your alias and then [click here](#) to connect to your personal e-mail account.

Public Access [Click here](#) to: browse Public Folders, find names in the Address Book, and post messages anonymously.

Yellow Lock at bottom right of website

Emails

- SPAM emails are becoming easier to detect by the average user. Look for these clues to identify SPAM:
 - The receiver's name is the same as the sender's
 - The subject is offering money making deals
 - The user is unknown and there are links to what appear to be legitimate websites.



Cyber crime: Laws in the Caribbean.

- On December 18th 2009 Jamaica moved its Cyber Crime bill into law making it possible to prosecute Cybercrime offenders.

Cyber crime: Laws in the Caribbean

- In Jamaica a case of a 26-year-old computer science student, who has been hauled before the Courts for allegedly hacking into the system of telecoms giant Digicel and stealing more than \$10 million in calling credit. Martin was charged with three counts of simple larceny and one count of conspiracy to defraud due to the lack of cyber crime legislation under which he could be prosecuted.

Cyber crime: Grenada Laws

- To date Grenada has no Cybercrime Legislation.

- What is used?
 - Criminal Code
 - Evidence act
 - Proceeds of Crimes

Are there methods to ensure adherence to data access norms for employees?

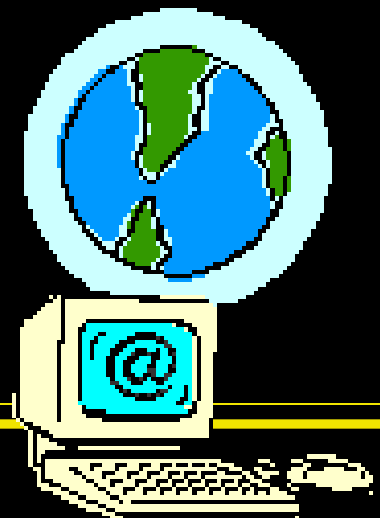
- Each organization must have a well-defined IT use policy. It is important to offer written description of the limits each employee needs to follow. They should also be told the legal consequences of any breach of the access norms.

Prevention Methods

- Prevent is always better than hours of frustration and lost of data
 - Frequent password changing
 - Safe Surfing
 - Frequent Virus Checks
 - Email Filters

Conclusion

- The key to protecting yourself is being aware.
- Not all cybercriminals are “hackers.”
- There is a whole other world that exists in cyberspace...make sure that your information travels safely.



Thank you