More and more Americans are adopting new and innovative technologies and spending more of their time on line. Our thirst for computers, smartphones, gadgets and WiFi seems to have no limits. At home, at work and at school, our growing dependence on technology, coupled with increasing cyber threats and risks to our privacy demands greater security in our online world. (Department of Homeland Security, 2013)

"Some of the greatest assets one can have are strong cybersecurity skills. Without them, anyone can fall prey to fraud and identity theft. One example is with the use of "free" WiFi. Though almost all young adults use smart-phones, most are unaware of the dangers associated with connecting to free WiFi and/ or access unsecured Websites. Once clicking "yes" to the terms and conditions on an unsecured network at the airport, coffee shop, mall or somewhere else, it becomes possible for cyber criminals to download everything from that smartphone." (Dr. Lee, 2014)

In Collaboration With:

![Collaboration Logo]

10 Skills U must know!
**Threat #1:** Browsing non-reputable/non-secured Websites

**Skill #1:** Preventing malware via non-secure Websites

**Threat #2:** Free non-reputable/non-secured WiFi network

**Skill #2:** Preventing Personal Identifiable Information (PII) theft via access to non-secure networks
**Threat #3:** Revealing confidential digital information to unauthorized individuals

**Skill #3:** Preventing the leaking of confidential digital information to unauthorized individuals

**Threat #4:** Malware via e-mail attachment

**Skill #4:** Preventing malware via e-mail attachment
**Threat #5**: ‘Friending’ unknown individual/account on social media

**Skill #5**: Preventing PII theft via social networks

**Threat #6**: Writing down personal passwords in visible places

**Skill #6**: Preventing unauthorized information system access via password exploitations
Threat #7: E-mail phishing

Skill #7: Preventing PII theft via e-mail phishing

Threat #8: Use of unknown USB or storage drive/device

Skill #8: Preventing information system compromise via USB or storage drive/device exploitations
**Threat #9:** Purchasing from non-reputable/non-secured Websites

**Skill #9:** Preventing credit-card information theft by purchasing from non-secured Websites

**Threat #10:** Failing to lock or log out of workstations when leaving work area

**Skill #10:** Preventing unauthorized computer system access via workstations lock or log out
Video...

Mobile CyberSecurity.mp4
The Realities of Cybercrime
Cybercrime is all in its many forms—e.g., online identity theft, financial fraud, hacking, phishing, and e-mail spoofing. Information privacy and property, including but not limited to, names, credit cards, and passwords, are all vulnerable to cybercrime. The losses can be financial, and potentially irreparable to an individual or company.

SHOULD I REPORT CYBERCRIME?
Cybercrime can be particularly difficult to investigate and prosecute. Be aware of legal and jurisdictional differences in computer crime.

Who to contact:
Local law enforcement. Even if you have been the target of a computer crime, your local law enforcement agency has an obligation to assist you, take your report, and refer you to other agencies.

FTC: The Internet Crime Complaint Center (IC3) is a partnership between the Federal Bureau of Investigation and the National White Collar Crime Center. Complainants may file online at: www.ic3.gov.

Federal Trade Commission: The FTC does not receive individual consumer complaints, but does operate the Consumer Sentinel, a database that is used by civil and criminal law enforcement agencies worldwide. File your complaint at: www.consumer.gov/ftc/.

Your Local Victim Service Provider: Most communities in the United States have victim advocates ready to help following a crime. File your victim service provider here: www.ojp.usdoj.gov/ot/vstable/index.aspx.

COLLECT AND KEEP EVIDENCE
It is important to keep any evidence you may have related to your complaint. Evidence may include the following:
- Canceled checks
- Credit card or other related receipts
- Chain of ownership (e.g., e-mail, chatroom, etc.)
- Screen shots of conversations, receipts, and online purchases
- Logs of your activity
- Printouts or preferably electronic copies of all emails (forwarded, include full email header information)
- Printouts or preferably electronic copies of web pages
- Phone records

TIPS FOR SPECIFIC TYPES OF CYBERCRIME
These are useful tips to follow for some specific types of cybercrime:

In cases of identity theft:
- Make sure you change your passwords for all online accounts: bank, credit card, and mobile, and any service that requires a login.
- Use strong and unique passwords, and numbers and symbols.
- Clean any unauthorized or compromised credit or bank accounts: inform the companies that someone may be using your identity, and find out if there have been any unauthorized transactions.

Think about what other personal information may be at risk. You may need to contact other agencies depending on the type of theft.

File a report with your local law enforcement agency. You will need to provide a copy of the law enforcement report to your bank, creditors, or businesses, credit bureaus, etc.

OTHER RESOURCES OR FILE A COMPLAINT
- Consumer complaint: www.consumer.gov/file-a-complaint.html
- Cyber-Watch, operated by the National Center for Missing & Exploited Children: www.cyberwatch.gov
- The Surface Test Laboratory: www.cslabs.org
- U.S. District Court: www.uscourts.gov.

How Did This Happen to Me?
A Word about Malware:
Avoid malware with the following tips from the STOP. THINK. CONNECT. campaign:
- Keep a clean computer: by making sure your security software, operating system, and web browser are up to date.
- Use antivirus, firewall, and other security software.
- Be aware of online fraud and phishing.
- Protect your personal information.
- Use strong and unique passwords.

If your personal information has been stolen through a corporate data breach, you will likely be contacted by the business or agency, whose data was compromised with additional instructions, as appropriate.

If a data breach occurs, contact one of the three credit bureaus to request a fraud alert (Equifax at 1-800-525-6285, Experian at 1-888-397-3742, or TransUnion at 1-800-680-1111). Request that the credit bureau place a fraud alert on your credit report to prevent any further fraudulent activity occurring. As soon as one of the bureaus issues a fraud alert, the other two bureaus are automatically notified.

In cases of Social Security fraud:
If you believe someone is using your social security number for employment purposes or to fraudulently receive Social Security benefits, contact the Social Security Administration’s Hotline at 1-800-342-3974. Request a copy of your Social Security statement to verify its accuracy.

In cases of online stalking:
In cases where the offender is known, send the stalker a clear written warning stating the contact is unwelcome and asking that the perpetrator cease sending communications of any kind.

Save copies of all communication from the stalker, including emails, threatening messages, messages via social media, and document each contact, including dates, times, and additional contact information, when appropriate.

File a complaint with the U.S. Postal Service (USPS) and your local law enforcement. If you have not already done so, file a complaint with your local law enforcement.

Maintain your online presence. Set security and privacy settings on social networking sites and other services to your comfort level of sharing.

Check the websites of the companies and service providers that you use. They may have information on how to protect yourself.

Consider changing your email address and IP address to protect yourself.

Make sure you change your passwords for all online accounts: bank, credit card, and mobile, and any service that requires a login.

Use strong and unique passwords, and numbers and symbols.

Clean any unauthorized or compromised credit or bank accounts: inform the companies that someone may be using your identity, and find out if there have been any unauthorized transactions.

Think about what other personal information may be at risk. You may need to contact other agencies depending on the type of theft.

File a report with your local law enforcement agency. You will need to provide a copy of the law enforcement report to your bank, creditors, or businesses, credit bureaus, etc.

If your personal information has been stolen through a corporate data breach, you will likely be contacted by the business or agency, whose data was compromised with additional instructions, as appropriate.

If a data breach occurs, contact one of the three credit bureaus to request a fraud alert (Equifax at 1-800-525-6285, Experian at 1-888-397-3742, or TransUnion at 1-800-680-1111). Request that the credit bureau place a fraud alert on your credit report to prevent any further fraudulent activity occurring. As soon as one of the bureaus issues a fraud alert, the other two bureaus are automatically notified.

In cases of Social Security fraud:
If you believe someone is using your social security number for employment purposes or to fraudulently receive Social Security benefits, contact the Social Security Administration’s Hotline at 1-800-342-3974. Request a copy of your Social Security statement to verify its accuracy.

In cases of online stalking:
In cases where the offender is known, send the stalker a clear written warning stating the contact is unwelcome and asking that the perpetrator cease sending communications of any kind.

Save copies of all communication from the stalker, including emails, threatening messages, messages via social media, and document each contact, including dates, times, and additional contact information, when appropriate.

File a complaint with the U.S. Postal Service (USPS) and your local law enforcement. If you have not already done so, file a complaint with your local law enforcement.

Maintain your online presence. Set security and privacy settings on social networking sites and other services to your comfort level of sharing.

Consider changing your email address and IP address to protect yourself.

Make sure you change your passwords for all online accounts: bank, credit card, and mobile, and any service that requires a login.

Use strong and unique passwords, and numbers and symbols.

Clean any unauthorized or compromised credit or bank accounts: inform the companies that someone may be using your identity, and find out if there have been any unauthorized transactions.

Think about what other personal information may be at risk. You may need to contact other agencies depending on the type of theft.

File a report with your local law enforcement agency. You will need to provide a copy of the law enforcement report to your bank, creditors, or businesses, credit bureaus, etc.

Other resources or file a complaint:
- Better Business Bureau: www.bbb.org
- Consumer complaint: www.consumer.gov/file-a-complaint.html
- Cyber-Watch, operated by the National Center for Missing & Exploited Children: www.cyberwatch.gov
- The Surface Test Laboratory: www.cslabs.org
- U.S. Department of Justice (USDOJ): www.cybersafety.gov
- U.S. District Court: www.uscourts.gov
- U.S. Postal Service: www.usps.com

The National Center for Missing & Exploited Children helps to locate the nation’s missing children and to prevent further child abduction and victimization. Call the NCMEC at 1-800-843-5678.

Tips and Advice
If you are a victim of cybercrime, it is important to take steps to mitigate the damage and prevent further harm. Here are some tips:
- Change your passwords:
- Turn off your device:
- Secure your accounts:
- Report the incident:
- Take legal action:
- Seek support:
- Prevent future harm:

StaySafeOnline.org
Tips and Advice
IF YOU BECOME A VICTIM OF CYBERCRIME
- Better Business Bureau: www.bbb.org
- Consumer complaint: www.consumer.gov/file-a-complaint.html
- Cyber-Watch, operated by the National Center for Missing & Exploited Children: www.cyberwatch.gov
- The Surface Test Laboratory: www.cslabs.org
- U.S. Department of Justice (USDOJ): www.cybersafety.gov
- U.S. Postal Service: www.usps.com

The National Center for Missing & Exploited Children helps to locate the nation’s missing children and to prevent further child abduction and victimization. Call the NCMEC at 1-800-843-5678.

Tips and Advice
IF YOU BECOME A VICTIM OF CYBERCRIME
- Better Business Bureau: www.bbb.org
- Consumer complaint: www.consumer.gov/file-a-complaint.html
- Cyber-Watch, operated by the National Center for Missing & Exploited Children: www.cyberwatch.gov
- The Surface Test Laboratory: www.cslabs.org
- U.S. Department of Justice (USDOJ): www.cybersafety.gov
- U.S. Postal Service: www.usps.com

The National Center for Missing & Exploited Children helps to locate the nation’s missing children and to prevent further child abduction and victimization. Call the NCMEC at 1-800-843-5678.
Session 2
Questions?