CUSTOMER INFORMATION SECURITY AWARENESS TRAINING

INTRODUCTION

This course is designed to provide you with the knowledge to protect your personal and mostly financial information and sensitive data from cyber threats.

In your daily activities, you routinely provide sensitive data like names, Social Security numbers, and other confidential records to successfully carry out your day-to-day activities.

YOU are critical to the defense and protection of sensitive information systems and data. You will be well equipped to protect the sensitive data by incorporating the information technology security objectives learned in this presentation into your daily activities.

IN THESE TIMES OF GREAT CHANGE

- Change Your Perception
  Security is a necessity - not a burden.
- Be a Learner
  Understand security threats and vulnerabilities.
- Be Proactive
  Adopt good security habits.
- Seek Help and Advice
  Advanced technologies require educated users.

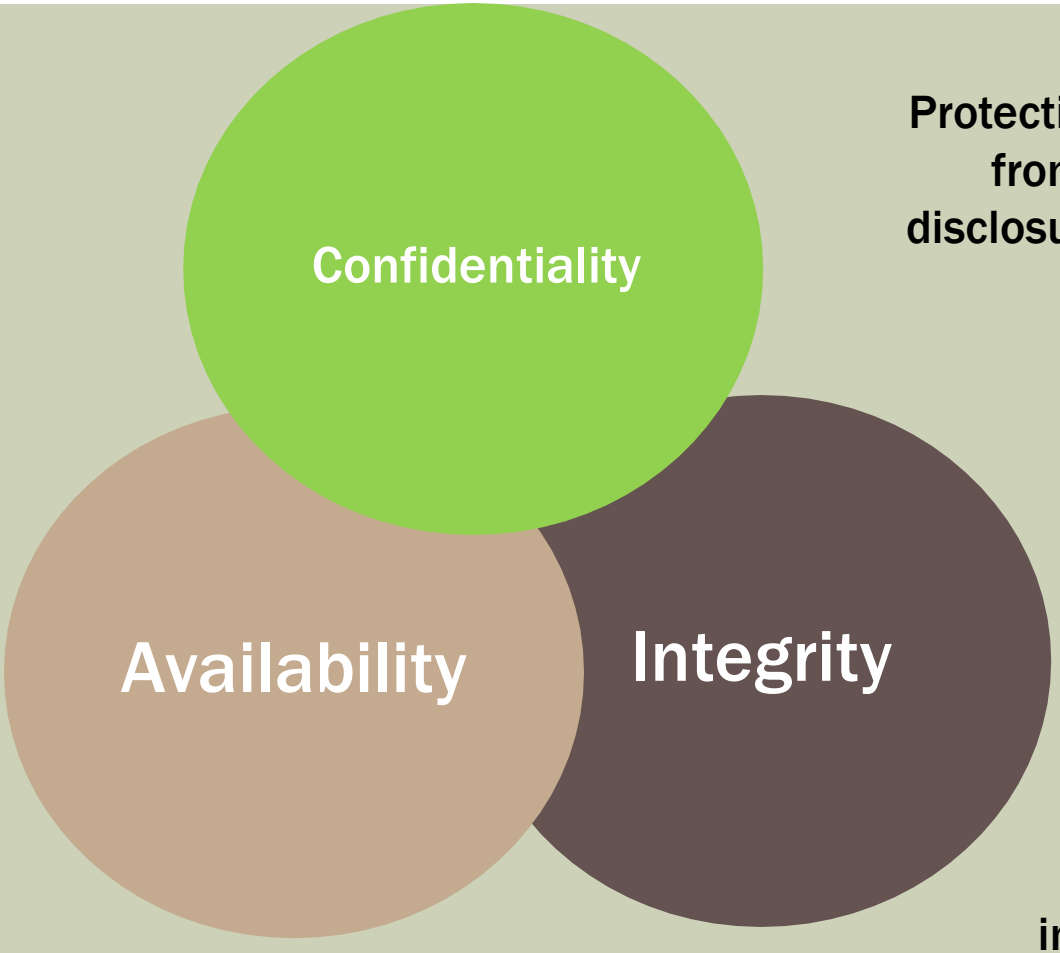
Information Security is YOUR responsibility.

WHAT IS INFORMATION SECURITY?

Information Security (IS) – The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

- Information security is achieved through implementing technical, management, and operational measures designed to protect the confidentiality, integrity and availability of information.
- The goal of an Information Security Program is to understand, manage, and reduce the risk to information under the control of the organization.

THE CIA CONCEPT



Protecting information from unauthorized disclosure to people or processes.

Defending information systems and resources from malicious, unauthorized users to ensure accessibility by authorized users.

Assuring the reliability and accuracy of information and IT resources.

CIA

Your bank ATM is a good example of an information system that must be confidential, available, and have integrity.

- Imagine if your account was not kept confidential and someone else was able to access it when they approached the ATM. How much damage could be done?
- Imagine if every time you went to the ATM, the balance it displayed was inaccurate (integrity). How could the poor integrity of your balance information adversely affect your account management?
- Imagine if your bank's ATM was rarely available when you needed it. Would you continue to use that bank?

DEFINING IT SECURITY

IT security is about protecting information assets by effectively managing risks. How much protection depends on the risk and magnitude of harm that could result if the data were lost, misused, disclosed, or modified.

Assets are computers and data.

Risks are managed by evaluating:

- Vulnerabilities - Weaknesses in a computer or network that leave it susceptible to potential exploitation such as unauthorized use or access.
- Threats - the means through which a weakness can be exploited to adversely affect a network or supported systems.

WHAT IS A COMPUTER INCIDENT?

Computer incidents include compromised systems, attacks made on or from the Bank's computers, illegal or inappropriate use, and abuse of computer privileges. As soon as possible, report these incidents to the appropriate personnel.

Examples of computer incidents:

- You think someone is using a computer without authorization.
- Your files look like someone has been tampering with the data.
- Sensitive information has been disclosed.
- Your computer is acting strange.

INFORMATION SECURITY POLICY AND GOVERNANCE

- Federal regulations require all users of information technology systems to conform with certain basic requirements and receive annual IT security awareness training

- GLBA - The Gramm–Leach–Bliley Act requires financial institutions to maintain procedures that protect consumers' personal financial information

WHAT IS A CYBER ATTACK?

A malicious attempt to undermine or compromise the function of a computer-based system, or attempt to track the online movements of individuals without their permission.

- Attacks are Pervasive and Common
  - The Department of Defense (DoD) detects three million unauthorized "scans"- or attempts by possible intruders to access official networks every day.
- Attacks Can be Costly
  - The Ponemon Institute benchmarked 50 organizations - the median annualized cost of a cyber attack is $5.9M/year.
- Attacks Don't Have to be Costly
  - According to the Ponemon Institute, a strong security posture moderates the cost of cyber attacks.

PREVENTING CYBER ATTACKS

Information assets have become a great source of value and wealth for individuals with malicious intent. Cyber attacks are a dangerous threat to the networks and data, however there are so me steps you can take to prevent them.

- Ensure that anti-virus software and patches are up to date on al l computers and laptops.
- Ensure that laptops and mobile devices are encrypted with trusted software.
- Never share passwords with anyone.
- Be vigilant about slow running applications. It could be a sign of a computer virus.

CURRENT & EMERGING CYBER THREATS

- Hostile attacks designed to establish a foothold within the infrastructure of target organizations remain the most serious cyber threat. Exfiltration of data through these attacks has been characterized as the biggest transfer of wealth in terms of intellectual property in history.

- Mobile device security represents an unprecedented layer of complexity and connectivity. Smart phones are powerful, ubiquitous and have exceeded the sales of PCs. They have become the most popular means to access the Internet. Attackers see them as a gateway into networks to access sensitive data.

- Clouds offer substantial gains for cost savings, productivity and security; however they are also attractive targets for attackers. Clouds represent another alternative to hosting an application and storing data, and must be secure.

COMMON CYBERSECURITY THREATS

- Malware
- Viruses
- Insider threats
- Spyware
- Hackers
- Theft or loss of sensitive data
- Internet and email scams
- Phishing
- Identity theft

CYBER CRIME

Cyber crime refers to any crime that involves a computer and a network. Offenses are primarily committed through the Internet.

- Common examples of cyber crime include:
  - Credit card fraud,
  - Spam, and
  - Identity theft.
- Information and information system assets from financial institutions are a high value target.
- Criminals, terrorists, and nation states with malicious intent work daily to steal, disrupt, and change information systems at financial institutions.

PASSWORDS

A strong password for your network account and other applications is a basic protection mechanism.

- Two rules for stronger passwords:
  - Create a password at least eight characters in length.
  - Password should contain at least one each:
    - Capital letter
    - Lowercase letter
    - Number
    - Special character (%,^,*,?)

- Use a passphrase.
  - Use the initials of a song or phrase to create a unique password
  - Example: “Take me out to the ballgame!” becomes “Tmo2tBG!”
- Commit passwords to memory.
- DO NOT keep passwords near your computer or on your desk.

PASSWORD PROTECTION TIPS

- Change passwords often. Most applications will remind you to do this but if not, set up a reminder in your calendar at least every 60 days.
- Change password immediately if you suspect it is compromised.
- Create a different password for each system or application.
- Do not reuse passwords.
- Do not use generic information that can be easily obtained like family member names, pet names, birth dates, phone numbers, vehicle information, etc.
- NEVER share your password with anyone.

TAILGATING

When an unauthorized person follows someone to a restricted area without the consent of the authorized person.

- Never allow anyone to follow you into a secure area without proper authorization.
- Be aware of procedures for entering a secure area, securing your workstation when you leave the office, and securing your workstation during emergencies.
- Do not be afraid to challenge or report anyone who does not appear to be an authorized individual/visitor.
- Escort visitors to and from your office and around the facility.
- Report any suspicious activity to the proper personnel.

PHYSICAL SECURITY PROTECTION TIPS

- Lock your computer when it is not in use by using CTRL+ALT+DEL.
- Store and transport removable media such as CDs, DVDs, flash drives, and external hard drives in a secure manner to prevent theft or loss.
- Only connect bank-authorized removable media devices.
- Encrypt all devices which contain sensitive information.
- Keep sensitive information out of sight when visitors are present.
- Quickly retrieve faxes and print jobs containing sensitive information.

EMAIL SECURITY

- Emails that contain sensitive data must be encrypted before being sent.

SOCIAL ENGINEERING

These individuals may look trust worthy, but in fact are sophisticated cyber criminals. They use social engineering techniques to obtain your personal information, access sensitive government information, and even steal your identity.

SOCIAL ENGINEERING

- Social engineering is classically defined as the art of manipulating and exploiting human behavior to gain unauthorized access to systems and information for fraudulent or criminal purposes.
- Social engineering attacks are more common and more successful than computer hacking attacks against the network.
- Social engineers will gain information by exploiting the desire of humans to trust and help each other.
- Criminals can bypass network firewalls and building access systems to steal data and disrupt operations with a successful social engineering attack.

SOCIAL ENGINEERING

Social engineering attacks are based on natural human desires like:

- Trust
- Desire to help
- Desire to avoid conflict
- Fear
- Curiosity
- Ignorance and carelessness

SOCIAL ENGINEERING

Social engineers want any information that will give them access to secure systems or facilities. Common targets are:

- Passwords
- Security badges
- Access to secure areas of the building
- Smart phones
- Wallets
- Personal information

COMBAT SOCIAL ENGINEERING

- Be careful about discussing work, your family, or personal information in public. You never know who is listening.
- Be cautious of the personal information that you share on social media sites like Facebook. Criminals can use the information you post in a social engineering scam.

PHISHING ATTACKS

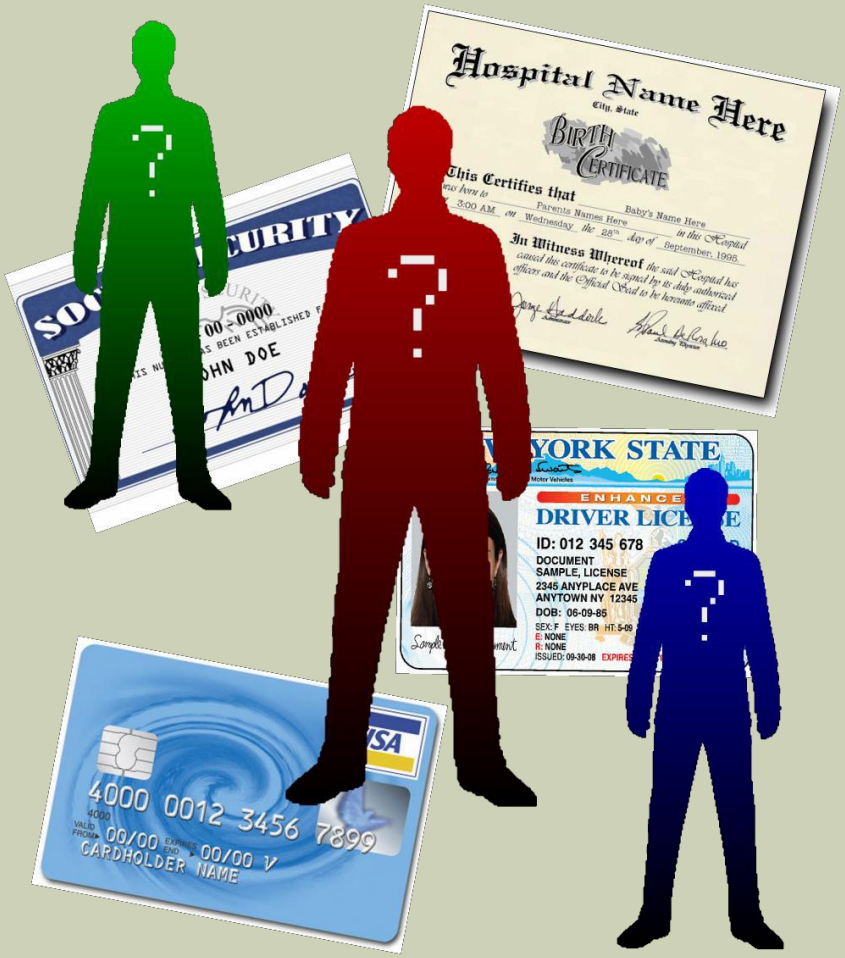
- Phishing is a social engineering scam whereby intruders seek access to your personal information or passwords by posing as a legitimate business or organization with legitimate reason to request information.
- Usually an email (or text) alerts you to a problem with your account and asks you to click on a link and provide information to correct the situation.
- These emails look real and often contain the organization's logo and trademark. The URL in the email resembles the legitimate web address. For example "Amazons.com".
- Spear phishing is an attack that targets a specific individual or business. The email is addressed to you and appears to be sent from an organization you know and trust, like a government agency or a professional association.
- Whaling is a phishing or spear phishing attack aimed at a senior official in the organization.

COMBAT PHISHING

- NEVER provide your password to anyone via email.
- Be suspicious of any email that:
  - Requests personal information.
  - Contains spelling and grammatical errors.
  - Asks you to click on a link or image or open an attachment.
  - Is unexpected or from a company or organization with whom you do not have a relationship.
- If you are suspicious of an email:
  - Do not click on the links provided in the email.
  - Do not open any attachments in the email.
  - Do not provide personal information or financial data.
  - Do not forward the email.
  - Delete it from your Inbox.

IDENTITY THEFT

- The Federal Trade Commission estimates that 9 million people have their identity stolen each year.
- Identity thieves use names, addresses, Social Security numbers, and financial information of their victims to obtain credit cards, loans, and bank accounts for themselves.



PREVENTING IDENTITY THEFT

- Be cautious when providing your Social Security number. Know how and why it will be used.
- Review credit card and bank statements at least monthly for unauthorized transactions.
- Use strong passwords for your home computer and web sites you visit, especially email accounts and financial institutions.
- Leave your Social Security card and passport at home. Never leave them in your purse or wallet unless necessary.
- Shred sensitive documents and mail containing your name and address.

MALWARE

- Malware (short for malicious software) does damage to, steals information from, or disrupts a computer system.
  - Malware is commonly installed through email attachments, downloading infected files, or visiting an infected web site.
  - It can corrupt files, erase your hard drive, or give a hacker access to your computer.

COMBAT MALWARE

- Scan attachments with antivirus software before downloading. Do not trust any attachments, even those that come from recognized senders.
- Delete suspicious emails without opening them.
- If you believe your computer is infected, contact the appropriate IT personnel.

SECURITY OUTSIDE OF THE OFFICE

- Security researchers say that 35% of data breaches at U.S. companies are caused by losing laptops or other mobile devices.

- Be vigilant about protecting information and information systems outside of the home or office.

MOBILE DEVICE LOSS AND THEFT

Cyber attacks are a dangerous threat to the Bank's networks and data, however a large number of breaches occur because of loss or theft of mobile devices.

- Never leave laptops, cell phones, or other mobile devices unattended – especially when travelling.
- Ensure that the wireless security features are properly configured.
- When away from your desk, use a computer lock for your laptop or place it in a locked cabinet.
- Mobile devices that contain Personally identifiable information must be encrypted.
- Report lost or stolen devices immediately.

PERSONALLY IDENTIFIABLE INFORMATION

- Personally identifiable information (PII) can be used to distinguish or trace someone's identity, or can be linked to a specific individual.
- Any such item of information can be PII, including:
  - Sensitive data - financial or legal information;
  - "Neutral" information - name, facial photos, work address; or
  - Contextual information - file folder for a specific customer that contains a list of account numbers.
- PII must be protected, whether in paper, electronic, or oral form.
- Seemingly innocuous information can identify an individual when combined with other data or compared to a data set that includes other PII.

COMMON EXAMPLES OF PII

- Name
- Social Security number (SSN)
- Date of birth (DOB)
- Mother's maiden name
- Financial records
- Email address
- Driver's license number
- Passport number

- Safeguard personal information in your possession, whether it be in paper or electronic format.
- Report suspected privacy violations or incidents.
- Shred documents containing PII; NEVER place them in the trash.

- Don’t leave documents that contain PII on printers and fax machines.
- Don’t leave files or documents containing PII unsecured on your desk when you are not there.
- Follow the technical, personnel, administrative, and telecommunication safeguards for computer systems you use.
- Take user awareness training annually.

COMMON SCENARIOS

Privacy incidents most often occur from:

- Loss, damage, theft, or improper disposal of equipment, media, or papers containing PII.
- Accidentally sending a file containing PII to a person not authorized to view the file or sending it in an unprotected manner (e.g., unencrypted).
- Allowing an unauthorized person to use your computer or credentials to access PII.
- Any security situation that could compromise PII (e.g., virus, phishing email, social engineering attack).

HOME SECURITY

- Many of the tips in this presentation can be used to protect your home computer.
- Criminals can use your personal information to steal your identity and ruin your finances.
- Protecting yourself and your family on the Internet at home is just as important as protecting information systems at work.

SAFEGUARD YOUR HOME COMPUTER

- Use passwords on personal computers and mobile devices.
- Install and update antivirus software on your home computer.
- Enable the firewall on your computer.
- Routinely backup your files.
- Follow the instructions in the user manual to enable encryption for your wireless router.

CONGRATULATIONS