CYBERSECURITY AWARENESS

Presented by: Islanders Bank
Cybersecurity Awareness

- Cybersecurity Awareness Objectives:
  - Define Cybersecurity & why it’s important
  - Provide information about Dept. Homeland Security Cybersecurity Campaigns:
    - National Cybersecurity Month, and
  - Review Current Cybercrime Trends and Threats
  - Explain the Threat Environment
    - Hardware, Software, Email, Web Browsing, Social Media, etc.
  - Provide Resources with Steps to Protect Yourself and Your Family Online
Cybersecurity Awareness

What is Cybersecurity?

- N.I.S.T.: “The process of protecting information by preventing, detecting and responding to attacks.”
  - N.I.S.T. framework for Cybersecurity: Identify, Protect, Detect, Respond and Recover

Why is Cybersecurity Necessary?

- Diligent cybersecurity is necessary because the risks and vulnerabilities – computer and human – along with advanced, persistent threat actors make the confidential, financial and personal information we possess an active and on-going target.
  - Threat actors = Internet crooks who are sophisticated, diligent and patient
  - Computer risks are program vulnerabilities exploited to execute malware
  - Human vulnerabilities are exposed via social engineering and phishing emails

Losing data, having data stolen, becoming the victim of a hacker or malware is not only an inconvenience but the financial, reputational and emotional experience can be overwhelming, and depending on the circumstances, devastating.

Our curiosity and trusting nature get A LOT of us in trouble!
Cybersecurity Awareness

- **Ongoing, Year-Round Security Awareness**
    - **Stop.** Before you use the Internet; understand the risks and potential threats
    - **Think.** How will your online activities impact your privacy, security and safety
    - **Connect.** Enjoy the Internet knowing you’ve taken steps to ensure a safe experience

- **Campaign goal**
  - Increase understanding of cyber threats
  - Empower American public to be safer and more secure online

- **October is National Cybersecurity Awareness Month**
  - Department of Homeland Security 2015 Cybersecurity Themes and Events

*Confidentiality, integrity and authenticity are not a given when using the Internet and, in most cases, all are absent!*
Trends in Cyber Crime

Current Cyber Crime Trends and Threats

- Targeted Attacks – Advanced Persistent Threats (APTs)
  - Specific Target (e.g. Home Depot & Sony security breaches)
  - Silence (e.g. Target)
  - Duration (e.g. The “Great Bank Heist of 2015”; attack lasted months using Carbanak malware)
  - “Hacktivism” - The act of hacking or breaking into a computer system for politically or socially motivated purposes

- Account Takeover
  - Cyber-thieves gain control by stealing valid online banking credentials
  - Corporate Accounts most common; provide access to payroll and pre-approved wire status & limits

- Malware
  - Malicious software intended to damage, disable or remotely control a computer or system examples include: Ransomware, Rootkits and Spyware

- Phishing Emails (e.g. IRS emails, UPS/FedEx)
  - A scam to acquire information such as user names, passwords, social security & credit card numbers by masquerading as a trustworthy entity
  - Executed via a malicious link or attachment contained in email
  - Poor grammar or spelling
  - Urgent Requests
  - Not a new trend & most common method for engaging in the tactics listed above
Trends in Cyber Crime

- **Current Cyber Crime Trends and Threats, cont.**
  - Escalation of ATM of POS Attacks
    - Great Bank Heist of 2015
    - Home Depot & Target Security Breaches
  - Virtual/Mobile Payment Systems (e.g. Square & iPay)
    - 2014 – 30% of merchants accepting mobile payments
    - 2014 – Mobile Commerce Transactions
      - Accounted for only 14% of Total Transaction Volume
      - Responsible for 21% of Fraud
  - Cyber criminals leveraging the deep web and dark net services to share and sell “crime-ware”
    - Online libraries & advertisements of stolen data
    - Training on phishing, key-logging and DDoS attacks
    - Recruitment of money mules
  - The “Internet of Things”
    - New categories of digital devices, from domestic appliances to home security and climate control, connected to and from the Internet
    - Devices will increasingly become targets as cyber criminals develop a business model to make money.
The Threat Environment
Scary Things Can Happen

- Any “connected” device is a potential risk!
  - As we connect more and more devices to the Internet for remote or cloud management, cybercriminals will continue to identify and exploit vulnerabilities.

- Unpatched computers create BIG risks
  - **What is a patch?** A fix to a program bug or vulnerability. A patch is an actual piece of object code that is inserted into an executable program (e.g. Internet Explorer, MS Word, MS Excel, etc.)
  - Patches are typically available as downloads from the Internet.
  - Recent data breaches exemplify the role of unpatched computers
    - 99% of computer exploits occur *more than a year after* vulnerability disclosed
    - 97% of exploits from just 10 unpatched vulnerabilities
  - When possible, **automate software updates**

- Everyday email use and web browsing expose us to threats
  - Phishing and SPAM attacks account for 70-80% of all email
    - Phishing accounts for 20% of recorded security incidents
    - With *alarming* response rates: 11% of recipients of phishing emails click on malicious attachments & links

*When it comes to phishing, YOU are the target NOT your computer!!!*
Scary Things Can Happen: Examples

- **Ransomware** - A type of malware that restricts access to a computer system that it infects in some method, typically email, and demands that the user pay a ransom to the operators of the malware to remove the restriction.
  - Two forms in circulation
    - Locker Ransomware – Denies access to computer or device
    - Crypto Ransomware – Denies access to files or data
  - Both types aimed squarely at our digital lifestyle and specifically designed to deny complete access to something we want or need.
  - Do NOT pay the ransom!
    - Examples:
      - CryptoLocker
      - Cryptowall
      - Reveton
      - TorrentLocker
Scary Things Can Happen: Examples

- **Distributed Denial of Service**
  - DDoS is a type of denial of service attack where multiple compromised systems, which are often infected with a Trojan, are used to flood traffic to a single system causing denial of access to something such as a website.

- **(DDoS) for Hire**
  - Hackers are openly competing to offer services that can take out a rival online business or settle a score.
  - According to Verizon’s latest Distributed Denial of Service Trends report, attacks can cost between $5 (USD) per hour or as low as $2 (USD) an hour.
  - Massive and longstanding attacks can be launched for as little as $800 a month.
Scary Things Can Happen: Examples

- **Surface Web, Deep Web & Dark Web – A Brief Explanation**
  - **Surface Web** = All *content* which can be *indexed* by a *search engine*
    - Search engines use links to navigate pages and create content indexes
  - **Deep Web** = *Content* which *search engines cannot index*
    - Search boxes and inquiries directly into a website
      - Government Databases & Libraries
  - **Dark Web** = *Portion of the deep web* which is intentionally hidden and requires a *special browser*

- **Websites that sell stolen card data are called “dumps”**

- **“McDumpals – i’m swipin’ it”**
  - McDumpals is an online site that, as of May 2014, was selling cards stolen from data breaches at main street stores in nearly every U.S. state!

- **Ashley Madison**
  - User data was “dumped” on to the dark web
Cybersecurity Best Practices: Personal & Business Computers

- **Antivirus Software**
  - Scheduled Definition Updates
  - Real Time File Scanning Enabled
  - Weekly FULL system scans

- **Computer Patching**
  - **What is Patching?**
    - Patching is the process of downloading and applying an application or service patch.
    - Patch management is the process of using a strategy and plan of what patches should be applied to which systems at a specified time.
    - Most application vendors recommend automatic updates.
Cybersecurity Best Practices: Personal & Business Computers

- **Strong Passwords**
  - The Longer the password, the Stronger the password
  - Do **NOT** use a dictionary word, family or pet name
  - Substitute numbers and special characters for letters
    - Examples: 7@lk!n6H3AD5; F\ee7w00&M@
  - Avoid re-using the same password for multiple systems
  - Use a Password Manager/Vault
    - KeePass
    - Dashlane
  - **HERE’S WHY:** Results from Target Breach:
    - Insecure file containing passwords saved on network
    - Weak and default passwords allowed Verizon security experts to assume role of network administrator with complete freedom to move about Target’s large network
    - 86%, or over 450,000 of Target’s 550,000 passwords were cracked
Cybersecurity Best Practices: Personal & Business Computers

- **Encryption**
  - The translation of data into a secret code
  - Requires secret key or password to open or read data
  - Unencrypted = Plain text
  - Encrypted = Cipher text
  - You should encrypt: Email, hard drives, backups and mobile devices

- **Malware Protection**
  - The **best protection** from malware continues to be the usual advice:
    - Be careful about what **email attachments** you open or links you click,
    - Be **cautious** when **surfing** and stay away from **suspicious websites** – don’t click on pop up ads
    - **Install** and maintain an updated, quality **antivirus** program.
  - Malware removal tools can remove more sophisticated files which have evaded antivirus detection
  - HERE’S WHY: Results from “Great Bank Heist”
    - Remote backdoor malware used to perform reconnaissance over several months
    - Information gathered allowed access to critical systems
    - Access gained allowed exploits of critical systems by impersonating the legitimate local user
Cybersecurity Best Practices: Personal & Business Computers

- **Trusteer Rapport**
  - Free download from [www.islandersbank.com](http://www.islandersbank.com)
  - Specifically targets financial malware
  - Examines critical Windows programming interfaces and blocks processes trying to intercept data
    - Keyloggers and Form Grabbers

- **Firewall**
  - Software or hardware which helps prevent hackers, and some types of malware, from getting to your computer through a network or the Internet.
  - Windows Firewall

- **User Account Controls (UAC)**
  - User Account Control is a feature in Windows that can help prevent unauthorized changes to your computer.

*A firewall isn’t the same thing as an anti-virus or anti-malware app. You need all three.*
Don’t be complacent - Mobile devices, smart phones & tablets, are susceptible to malware and viruses too!!!

Best Practices

- Choose your device carefully
- Protect with passcode
- Consider Anti-Virus or Anti-Malware
- Limit use of public Wi-Fi to secure networks only
- Turn on Encryption
- Utilize remote wipe capabilities
- Secure Bluetooth
  - Disable when not actively using and switch Bluetooth devices to hidden mode
- Stay current with “App” updates
  - Only download from a trusted “App Store” (e.g. iTunes or Google Play)
Cybersecurity Best Practices: Internet/Web Browsing

- **Practice Safe Browsing**
  - Protect your home wi-fi network with a password that only you and your family know
  - Don’t let your neighbors use your wi-fi connection
  - Don’t store your passwords in your web browser
  - Don’t click on pop-up ads or ads displayed on websites
  - Limit the use of Cookies
  - Try to limit your web browsing to sites that you’re familiar with or have prior knowledge of, and
  - If you usually browse the same websites everyday, be aware of subtle or obvious changes in appearance or text & images that seem out of place
    - Websites can be “spoofed”- designed to look the same as a legitimate website but are instead used to deliver malware or steal sensitive information
Cybersecurity Best Practices: Social Media

- **Social Media**
  - Websites and applications that enable users to create and share content or to participate in social networking
    - Don’t “Over Share”
      - Think before you share detailed information about yourself; could it be used to commit fraud?
      - Simple Google Search can return information shared on social media sites
    - Verify “Friend Requests”
      - Do you really know this person?
      - Does their profile seem legitimate?
    - Understand and Use Privacy Features & Settings
      - Consider making information like birthplace, birthday and employer “private”
      - You can control who sees your social media profile, photos and posts!
    - Select Strong Passwords
Cybersecurity Best Practices: Kids, Computers & the Internet

- Create separate user logon accounts for your children
- Don’t allow them to download or install software
- Use Windows Parental Controls
  - Set time limits on computer use
  - Limit games they play and programs they can run
- Configure Secure Internet Settings
  - Block based on content
  - Create an Approved Sites list, and
  - Set password so settings cannot be altered
- Monitor social media use
  - Be aware of who your child or children are engaging with online
Cybercrime Defenses & Responses

What to do if.....

Your computer becomes infected with a virus or malware
- Install Anti-virus software and run complete system scan
- Install one-time scanning tool and run complete scan
- Run malware scan
- Reboot into “safe mode” and run virus scan
- Revert to factory settings
- Seek professional help
- Do NOT pay ransom

Your financial information has been compromised: Online Banking Credentials, Credit Card Fraud
- Close your accounts immediately
- Contact Financial Institution(s)
- Contact Credit Reporting Agencies: Request Fraud Alert
- Order Credit Report
- Monitor Accounts

Always read your paper & electronic financial account statements promptly and carefully!
Cybercrime Defenses & Responses

- **What to do if.....**
  - **Your email or social media account are hacked**
    - Reclaim your account
    - Change your password
    - Enable two factor authentication
    - Check your email security settings
    - Scan your computer for malware
    - Notify your peers
    - Prevent it from happening again
  - **You become the victim of identity theft**
    - Contact Financial Institution(s)
    - Contact Credit Reporting Agencies: Request Fraud Alert & Free Credit Report
    - Report to FTC: Complete Online Complaint Form
    - File report with local police department
    - Consider adding Fraud Alert or Credit Freeze
Conclusion and Key “Take Aways”:

- Confidentiality, integrity and authenticity are not a given when using the Internet and, in most cases, all are absent!!
- Phishing is the most common method for cyber criminals to exploit or engage in online crime
  - Our curiosity and trusting nature get A LOT of us in trouble – THINK BEFORE YOU CLICK!!
  - YOU are the target NOT your computer!!!
- Anti-virus, Anti-Malware and Firewall = Best Security Defense
- Strong passwords stored in password manager = Best Security Practice
- Patch – keep systems and applications, including mobile, current
  - Schedule updates weekly
- Use Parental Controls
- Think about what you’re sharing online
- Always read your paper and electronic financial account statements promptly and carefully!
- Be Informed & Use Resources. **Stop. Think. And Connect Safely!!!!**
Cybersecurity Awareness

References

- Kaspersky Labs – Carbanak – APT, The Great Bank Robbery
- Krebs on Security
- BrightPlanet
- Welivesecurity – Cybercrime Trends and Predictions for 2015
- Sophos – Security Trends 2015
- Trend Micro – The Invisible Becomes Visible – Security Predictions for 2015 and Beyond