Protecting Yourself in Today's Cyber Landscape

May 2020

Presented by Don Boian,
Cybersecurity Outreach Director

Huntington
Welcome.®

Disclaimer

This presentation is intended for educational purposes only and does not replace independent professional judgment. Statements of fact and opinions expressed are those of the individual participants and, unless expressly stated to the contrary, are not the opinion or position of Huntington National Bank or its affiliates. Huntington does not endorse or approve, and assumes no responsibility for, the content, accuracy of completeness of the information presented. Professional assistance must be consulted prior to acting on any of the content in this presentation.

The Huntington National Bank is Member FDIC.

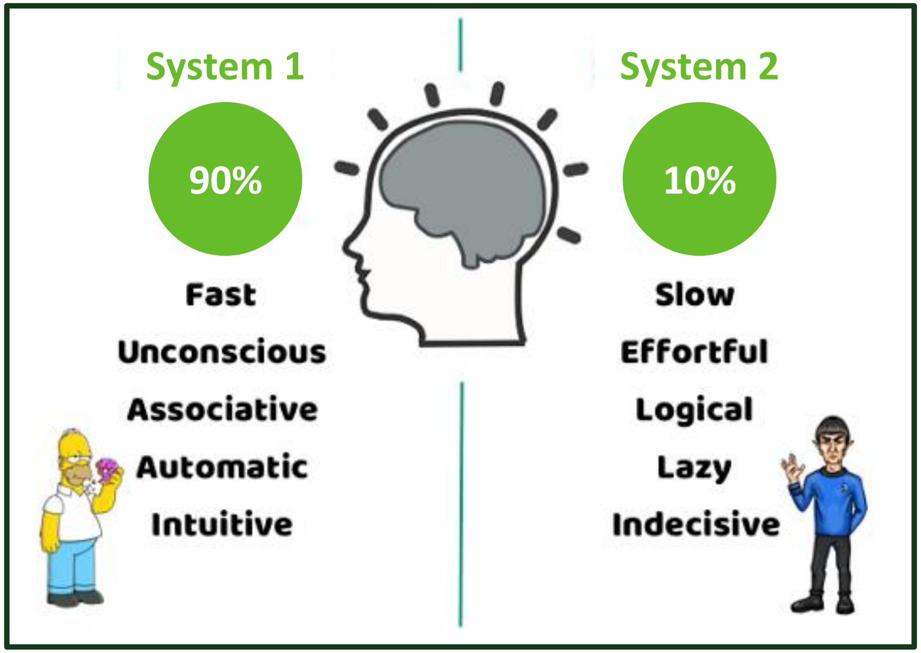
®, Huntington® and Huntington® are federally registered service marks of Huntington Bancshares Incorporated. ©2020 Huntington Bancshares Incorporated.

Welcome.

Why does Phishing work?

Psychology of Phishing

- Emotional Response vs. Logical Reasoning
- Fear
- High Anxiety Levels
- Distraction
- Information Overload



Source: http://www.allusanewshub.com/2020/03/07/designers-should-understand-users-make-most-decisions-without-rational-thinking/

Cybersecurity Employee Education

- Sensitive Information – How to mark it and protect it
- Privacy
- Phishing & Smishing awareness
- Social Engineering
- Current Threats & Scams
- Reporting Responsibilities

Your employees are your first line of cybersecurity defense!

Credential Security – Password Basics

- Chose a strong password/passphrase
- Change passwords regularly
- Never reuse passwords across multiple accounts
- Consider a password manager
- Change default passwords

Corporate Cybersecurity Basics*

Identify

- Inventory sensitive data (know where it is stored and processed, know what 3rd parties have your sensitive data)
- Inventory systems and software (necessary for Vulnerability Mgt, etc)
- Establish policies and procedures around Cybersecurity (WiFi, breach, etc)
- Independently assess your security and that of your 3rd parties

Protect

- Employee training/awareness (Phishing, BEC, Social Engineering, Fraud, …)
- Updated/Current OS and Applications (patch management)
- Practice good password management; Use Multi-factor Authentication
- Implement E-mail security (DMARC, SPF, DKIM), external banner, block spam/junk
- Backup data (conduct, maintain and test)

Detect

- Monitor your logs for anomalies (or outsource it – MSSP)
- Antivirus, Endpoint encryption, Data Loss Prevention - software up to date
- Increase network defensive barriers (Firewalls, IDS, IPS, …)
- Checks and Balances in ALL processes (Segregation of duties, least privilege, invoice/payment processing, …)
- Plan (and exercise) for the worst (malware, outage, breach, …)

Respond

- Establish and practice crisis management policies and procedures

Recover

- Cybersecurity Insurance – Purchase and/or update policies & know your coverage

* Start with these, but don't stop there once you've mastered them

BE BRILLANT AT THE BASICS

Personal Cybersecurity Basics*

1. Raise awareness (Phishing, Social Engineering, …) – know the threats
2. Passwords – NO reuse; Complex; Passphrase; Use a Password Manager
3. Backup data
4. Updated/Current OS and Applications – allow auto-update
5. Antivirus, Firewall, Home network – change default passwords!
6. Terms of Service; Beware of free services – YOU'RE the product
7. Geolocation/Location based services
8. Reputable applications and what they have access to
9. Home IoT Devices – Change default passwords; Security
10. WiFi Security
11. Credit Cards – Transaction Alerts (CNP); Use mobile app locking
12. Credit Reporting Bureaus - Freeze/Lock credit
13. Application Settings - Security & Privacy – periodically review/reset

BE BRILLANT AT THE BASICS

* Start with these, but don't stop there once you've mastered them

References

- Huntington - Privacy & Security
  - https://www.huntington.com/Privacy-Security
- FBI
  - Internet Crime Complaint Center (IC3)
    - https://www.ic3.gov/default.aspx
  - Public Service Announcements
    - https://www.ic3.gov/media/default.aspx
- Federal Trade Commission –
  - Cybersecurity for Small Business
    - https://www.ftc.gov/tips-advice/business-center/small-businesses/cybersecurity
  - Identity Theft
    - http://www.identitytheft.gov/
- NIST Cybersecurity Framework
  - https://www.nist.gov/cyberframework/framework
- Center for Internet Security
  - https://www.cisecurity.org/
- Cloud Security Alliance
  - https://cloudsecurityalliance.org/

References

- Credit Reporting Agencies
  - Equifax (888)766-0008 http://www.equifax.com/CreditReportAssistance
  - Experian (888)397-3742
    - Fraud - https://www.experian.com/fraud
    - Freeze - https://www.experian.com/freeze/center.html
  - TransUnion (800)680-7289
    - Fraud – https://www.transunion.com/solution/fraud-detection
    - Freeze - https://www.transunion.com/blog/identity-protection/credit-freeze-vs-credit-lock
- Federal Trade Commission – Complaint
  - http://www.ftc.gov/complaint

References – Cybersecurity Careers & Education

- Careers in Cybersecurity – CyberSeek
  - https://www.cyberseek.org/heatmap.html
  - https://www.cyberseek.org/pathway.html
- National Institute of Standards and Technology (NIST)

  National Initiative for Cybersecurity Education (NICE) Framework
  - https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework
- National Initiative for Cybersecurity Careers and Studies (NICCS)
  - https://niccs.us-cert.gov/
- STOP. THINK. CONNECT.
  - https://www.stopthinkconnect.org/
- FBI – Safe Online Surfing
  - https://sos.fbi.gov/en/