Cybersecurity

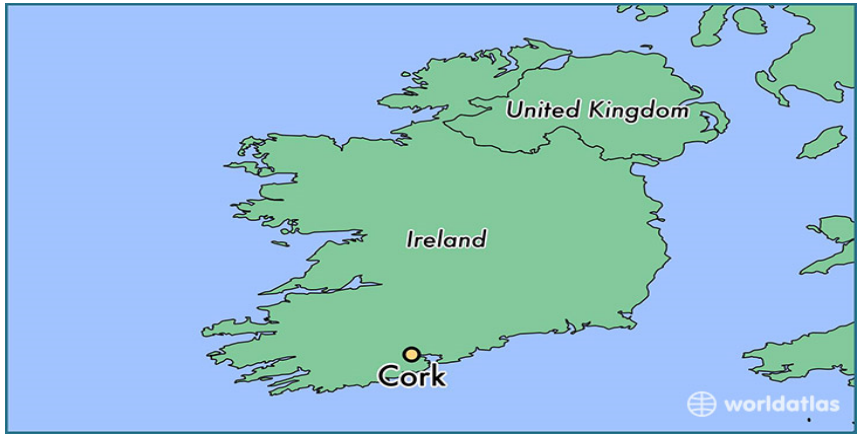
How to avoid scammers and some other possibly interesting topics

Brían McSweeney – April 2018

Agenda

- Introduction (Who even is this guy?)
- Cybersecurity – some definitions
- BIG topics in Cybersecurity
- OK, but WDIMTM (closer to home)
- Resources / Questions (the end is nigh)

Introduction



- Originally from Cork, Ireland

- Worked in Information Security and IT Risk for 17 years

- Currently working with a global financial institution (previously as a consultant in the Big 4)

- Lived in Beverly Shores since 2015

Cybersecurity definitions / topics / things you may have heard about!

- Computers and The Internet
- Digital Identity
- Authentication (and MFA or multi factor authentication)
- Internet of things
- Big Data
- The Cloud and cloud computing

Cyber or **Information Security** can be defined as the prevention of "bad things" happening to information or the systems that information happens to be living / travelling on. Often identified with the balanced protection of the **confidentiality**, **integrity** and **availability** of data (the C-I-A triad). Important to note balance - trade off between security and usability - in this definition.

The (cybersecurity) state we're in

- Data breaches (such as Equifax)
- Insiders, Snowden and the Shadow Brokers
- Nation State Threat Actors and Cyber Warfare
- Anonymous and other Hacktivist groups
- The Open Internet and Security
- Business Email Compromise
- Bitcoin, Cryptocurrency and Blockchain Technologies

What does it mean to me? (closer to home)

- Identity Theft
- Online Fraud
- Social Engineering
- Denial of service / ransomware and extortion attempts

Common scams

Frequent scam examples:

- The 419 (Advance Fee) Scam
- You've Been Pre-Approved!
- The Phishing Scam
- Disaster Relief Scams
- Travel Scams
- Debt Relief Scams
- Lottery Scam
- Fake Check/Money Transfer Scams

Other common scam types:

- Greeting cards
- Threats / extortion attempts
- Romance scams

- Fake antivirus
- Facebook (or other social media) impersonation
- Make money fast scams
- Bitcoin scams
- Job offer scams
- Loyalty scheme phishing scam
- IRS scams
- Delivery (Fedex, UPS etc) scams
- Medical Emergency scams

Others:

- Fake shopping websites
- Fake news scam
- SMS Scams (Smshing

What practical steps can I take?

- Security Checklist - Ten simple steps you can take to reduce your risk.
  1. Install up-to-date anti-virus and anti-spyware programs on your home computers.
  2. Use a personal firewall.
  3. Download security patches and software/operating system updates in a timely fashion.
  4. Use caution when using unsecure Wireless Hotspots, such as internet cafes or airports.
  5. Enable security features on your home wireless network and use a strong password or key to prevent unwanted access.
  6. Use strong passwords and keep them safe if you must write them down.
  7. Learn to identify and avoid Phishing and Spear Phishing e-mails.
  8. Review your financial statements as soon as they arrive for discrepancies or suspicious activity.
  9. Shred all documents with personal or financial information before disposal.
  10. Use care when participating in Social Networking sites, such as Facebook or LinkedIn. Do not reveal sensitive personal information, and modify your privacy settings to prevent strangers from viewing your pages.

Questions?

- Additional resources
  - https://www.justice.gov/criminal-fraud/identity-theft/identity-theft-and-identity-fraud
  - https://www.ssa.gov/pubs/EN-05-10064.pdf?bc=25395994
  - https://www.consumer.ftc.gov/topics/privacy-identity-online-security
  - https://www.investopedia.com/articles/personal-finance/040115/watch-out-these-top-internet-scams.asp
  - http://www.toptenreviews.com/software/privacy/best-personal-firewall-software/