

Regarding Cybercrime

Andy Davis, Oct 2022 Session

Presentation Outline

- ◇ Different types of cybercrime
- ◇ Reasons GE might be a victim
- ◇ Why it is difficult to prevent cybercrime
- ◇ Examples of cybercrime
- ◇ How to protect against cybercrime
- ◇ Resources

Different types of Cybercrime

- ◆ Phishing Scam
 - ◆ Fake emails to get personal information
- ◆ Website Spoofing
 - ◆ Fake websites that look like real login pages
- ◆ Ransomware
 - ◆ Steals services, asks for money in return to get access again
- ◆ Malware
 - ◆ Malicious software, or viruses
- ◆ Social engineering
 - ◆ More of person-to-person type of crime than cyber

Reasons GE might be a victim

- ◇ Rising company means bigger profits
 - ◇ Potential for Ransomware
- ◇ More employees means more data
 - ◇ Potential for Phishing Scams, Social Engineering
- ◇ Expansion might bring unsolicited emails for new products
 - ◇ Potential for Phishing Scams, Website Spoofing, Malware

Why it is difficult to prevent cybercrime

- ◆ Evolving technology invites evolving techniques for crime
- ◆ Software / Hardware become out of date faster than ever before
- ◆ 91% of cybercrime is due to Phishing Scams
 - ◆ Hard to tell fake emails on mobile devices
 - ◆ Customized fonts can hide typos
 - ◆ Lowercase L vs Uppercase i :: l vs I

Examples of cybercrime

- ◆ Twitch.tv 2021
 - ◆ 125 GB file was posted online, containing the following
 - ◆ The complete repository of Twitch.tv along with commit history
 - ◆ The source code for Twitch mobile, desktop, and gaming console apps
 - ◆ Twitch creators' earning details over three years
 - ◆ Twitch's internal security details and tools
 - ◆ Sensitive data on IGDB and CurseFrog, other software products owned by Twitch's parent company
 - ◆ The existence of an unreleased software by Amazon Game Studios for competing with Valve's Steam, titled Amazon Vapor
 - ◆ Twitch proprietary SDK code and internal AWS service data

Examples of cybercrime

- ◇ Twitch.tv, 2021
 - ◇ 125GB file was said to be one of many
 - ◇ Other files never got released, but potentially had account information
 - ◇ Resulted from obsolete code or dependencies
 - ◇ Top 10 threat of 2021
- ◇ (Kiuwan.com, 2021)

Examples of cybercrime

- ◆ Uber, 2022

- ◆ Uncertain what the hack got access to, but was certain they had access to:

- ◆ Slack messages

- ◆ Dashboard for security bugs and vulnerabilities

- ◆ Financial tools

- ◆ Potentially user accounts and bank information

- ◆ Some say intent was to sell, others say intent was to embarrass

Examples of cybercrime

- ◆ Uber, 2022
 - ◆ Type of Social Engineering: Exhaustion attack
 - ◆ Repeated messages to an employee email or phone
 - ◆ Eventually calls to say there is an issue and need access to account to resolve
 - ◆ Not a super technical hack, but super common
 - ◆ More so with people becoming remote or using other devices besides desktops/laptops as primary sources of access
- ◆ (Schneier, 2022), (Zetlin, 2022)

How to prevent against cybercrime

- ◆ Yearly, mandatory training
 - ◆ Included with other yearly trainings
 - ◆ Kept up to date on cybercrime trends
- ◆ Company emails should only be accessed on company hardware
 - ◆ Company computers and phones can be restricted and have protections installed
 - ◆ Similarly, access should only be allowed on a Private Network or VPN
- ◆ Have a way to report scam emails
 - ◆ IT Department to handle abuse

Resources

- ◇ BlueVoyant. (n.d.). *What is Cybercrime? Types and Prevention*. [online] Available at: <https://www.bluevoyant.com/blog/cybercrime-types-and-prevention>.
- ◇ Gannon, B (2022). *Topic 9 Lecture 3: Malware, cybercrime, and computer misuse*. [online] University of London. Available at: <https://learn.london.ac.uk/mod/page/view.php?id=98439>
- ◇ Kiuwan.com. (2021). *The Full Extent Of The Twitch Hack - Kiuwan*. [online] Available at: <https://www.kiuwan.com/blog/the-full-extent-of-the-twitch-hack/>.
- ◇ Schneier, B. (2022). *Opinion | The Uber Hack Exposes More Than Failed Data Security. The New York Times*. [online] 26 Sep. Available at: <https://www.nytimes.com/2022/09/26/opinion/uber-hack-data.html>.
- ◇ Zetlin, M. (2022). *Uber was hacked using a simple technique that might work on your company, too*. [online] Inc.com. Available at: <https://www.inc.com/minda-zetlin/uber-hack-multi-factor-authentication-mfa-vulnerability-phishing-exhaustion-attacks.html>.