JUNTO SERVICES • MARCH 2022
JUNTO SERVICES • MARCH 2022

CYBERSECURITY AWARENESS

Entrust Wealth Partners - Webinar Series

Jake Gord - Junto Services

JUNTO SERVICES

JUNTO SERVICES • MARCH 2022
JUNTO SERVICES • MARCH 2022

SIZE OF THE ISSUE

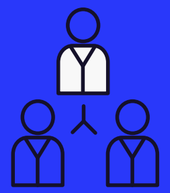
$20 BILLION

DAMAGES FROM CYBER ATTACKS IN 2021

CURRENT STATE

CYBER ATTACKS ON AN INDUSTRIAL SCALE

$102m in ransomware damages is accumulated each month



43% of cyberattacks target individuals and small businesses

One new cyber attack is attempted every 2 seconds

PERSONAL & BUSINESS TIPS

RANSOMWARE

- Ransomware is malicious software designed to restrict access to digital assets until a sum of money is paid.
  - Example - Colonial Pipeline
    - Ransomware breach that began through a chain email with NFSW(*not safe for work) images
- Vast majority of ransomware attacks start as simple Phishing attacks

PHISHING

- Phishing is a fraudulent email tactic that involves misrepresentation of the sender or reason for contact with the goal of receiving personal or confidential data from the recipient (i.e. account numbers, passwords, credit card #s, etc.)
- Ways to spot Phishing emails:
  - Poor Grammar
  - EMAIL HEADERS
  - Alerts from email provider
- Types of Phishing attacks: Smishing, Whale phishing, Spear phishing

PASSWORD MANAGERS

- The average person has more than 100 passwords in 2022.
- Using a password manager will help generate strong passwords automatically and store the info across devices
- Most Password Managers will alert you if one of your accounts has been found in a data breach
    - Change impacted passwords immediately if you receive this alert
- Avoid easy to guess password combinations such as "1Password", "LastPass", "Remember!"

IOT & ROUTER UPDATES

- IoT or "Internet of Things" devices are targets of regular cyber attacks
    - Ring Doorbells, routers, smart tv's, Alexa, etc.
- Change your standard passwords for these devices regularly, as they are easily overlooked and are usually set up with manufacturer defaults
- Updating these credentials will protect you from basic router attacks and "wardriving" (when hackers using scanning tools to identify and gain access to unsecure systems)

TRAVELING

- Avoid use of public wifi networks and charging ports
  - Instead, use mobile Wifi Hotspot
- Never plug an unknown or publicly available device into your phone or computer while traveling
  - Example - Stuxnet
    - Cyber attack started by Iranian scientists plugging in a USB drive they found in the parking lot that led to stalling their Nuclear Weapons Program

QR CODES

- DON'T SCAN UNKNOWN QR CODES
- QR Codes can lead to "dirty" websites or directly to malware
- The risk of QR codes far outweighs the benefit of using them

UPDATED OS/ ANTIVIRUS

- OS = operating system
- Update hygiene is key across all devices
- Windows and Mac have built in Antivirus that (if updated regularly) will keep you safe against the most common viruses/worms/trojans
- Phone OS updates are just as important as other device updates to protect against cyber attacks
    - Particularly important for Android users

AD BLOCKERS

- AdBlockers will help stop malicious tracking and scripts from executing on websites
- Even legitimate websites can have malicious AdCode installed
- Product examples: UBlock Origin, AdBlock

TWO-FACTOR AUTHENTICATION

- Two factor authentication is a method for gaining access to a system in which a user must successfully present two or more pieces of evidence to an authentication mechanism to log in.
  - Most applications utilize a password + text message (SMS) code
- #1 most cost effective thing an average person or business can do to protect their accounts
- Recommended to install on every account that you can
- If you own a business - make this your top Cybersecurity priority for 2022
- Product Examples: Duo Mobile/Okta

https://

- ALWAYS check the URL address of the websites you are visiting.
- Reputable sites should always begin with https://
  - The included "s" means you are visiting a secure website
- If a given website is http:// and unencrypted, there is a good chance it could be malicious.
  - User traffic and usage data is available in plain text to the public on unencrypted sites

ABOUT THE TEAM

JUNTO SERVICES

Jake Gord - Founder / CEO

Website: juntoservices.com

Email: jake@juntoservices.com

Phone: (256) 348-4532