Cybersecurity Awareness

RIGGS DISTLER
Since 1909
Mechanical-Electrical-Utility

AGENDA

- Impact
- IT Employee Policy
- IT internal Control Processes
- Passwords
- Phishing
- Spoofing – creating a fake email, account, or WIFI access
- Malware

AGENDA

- Ransomware
- Social Engineering
- WIFI (Public) – mobile data or VPN
- Connected Smart Devices and what can be exploited
- MFA/2FA
- CMMC – DoD
- Customers

IMPACT

- Q: What is the estimated global losses of cybercrime by the end of 2020, 2025?
- A: $1 Trillion USD
- A: $10 Trillin USD

- Q: What was the global spending for cybersecurity in 2004, 2020?
- A: $3.5 Billion USD
- A: $145 Billion USD

- Q: What was the estimated cost for ransomware attacks in 2015, 2020?
- A: $325 Million USD
- A: $11.5 Billion USD

HOW MANY DEVICES CONNECTED TO THE INTERNET

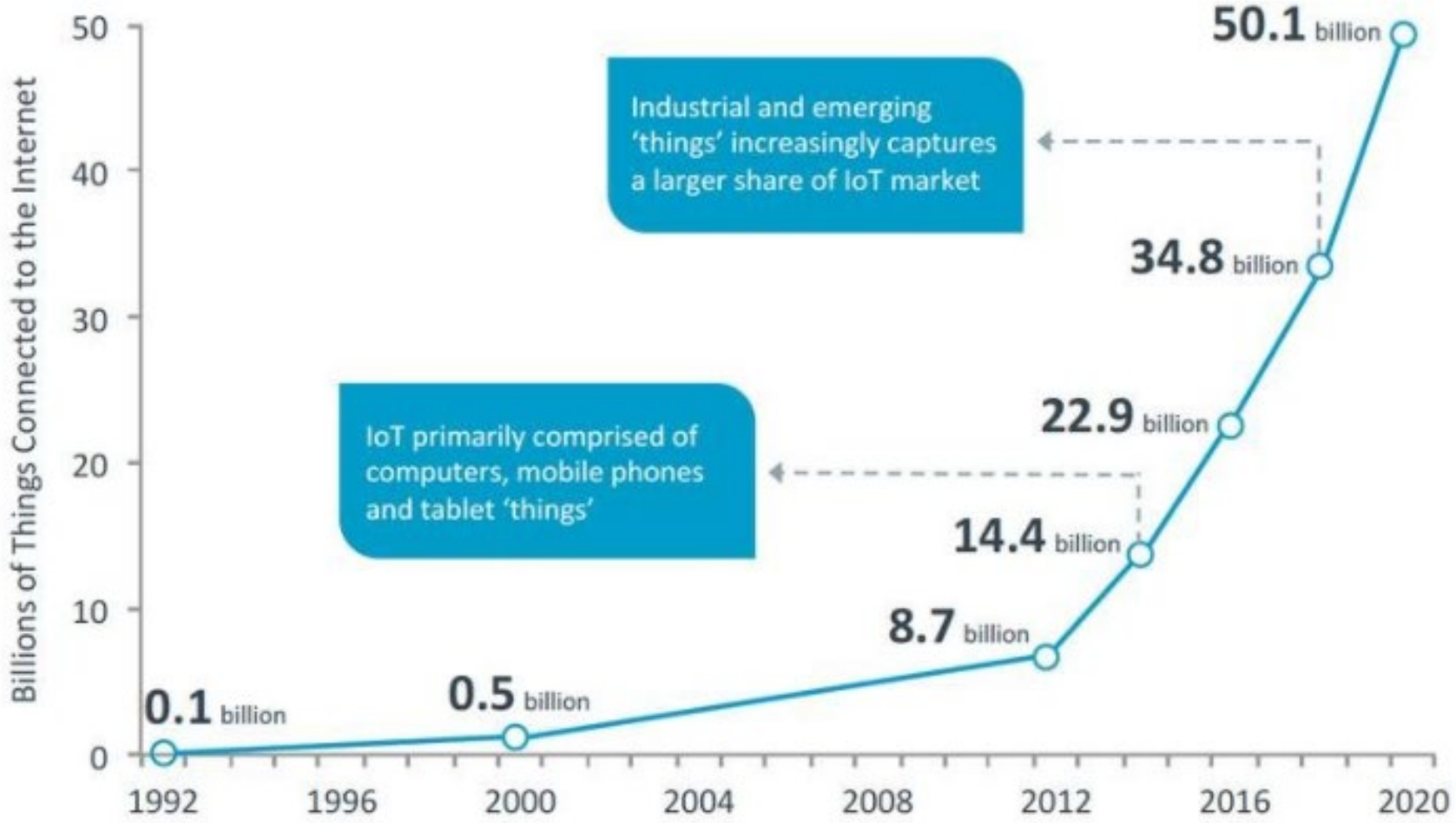
Q: Number of connected devices in 2015, 2020, 2025?

A: 15 billion

A: 25 billion

A: 40 billion

About 2007, there were more devices than people



PASSWORDS

Most Common Passwords:

- 123456
- 123456789
- Qwerty
- Password
- 12345
- Qwerty123
- 1q2w3e
- 12345678
- 111111
- 1234567890

Do you think the hackers know this?

PASSWORDS C0mpl3x1ty!

Password Reuse – we implement processes that limit the frequency of password reuse

Password Complexity – typically 8 characters

- 1 upper case letter
- 1 lower case letter
- 1 numeric
- 1 special character

Password Change Frequency – organizations typically force a change of a password every 60 to 90 days

Never Email passwords! You could type the wrong email address and send the email to the wrong person

EMAIL

- Estimated 90% of successful attacks are done through email
- Malicious files and links that ask for username and password
- Becoming more complex and effective through social engineering
- KnowBe4 – phishing tool that Riggs Distler uses
- [EXTERNAL] is in the subject line for email from outside of RDC
- Verify sender of an email – do you know this person and can you call them?
- Hover on links to see where they are coming from
- Report & escalate anything suspicious
- Do not open an attachment from an unknown sender
- Do not click on links from unknown senders
- If you do not know the source and cannot verify, notify IT

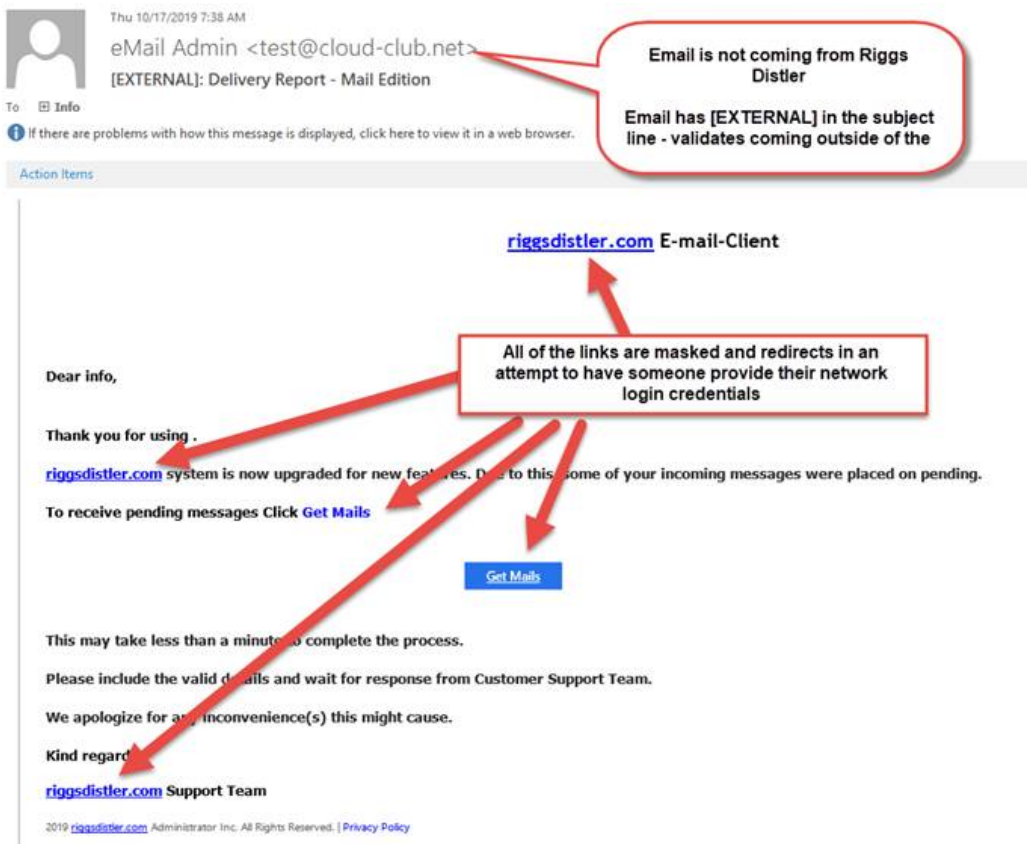
EMAIL PHISHING

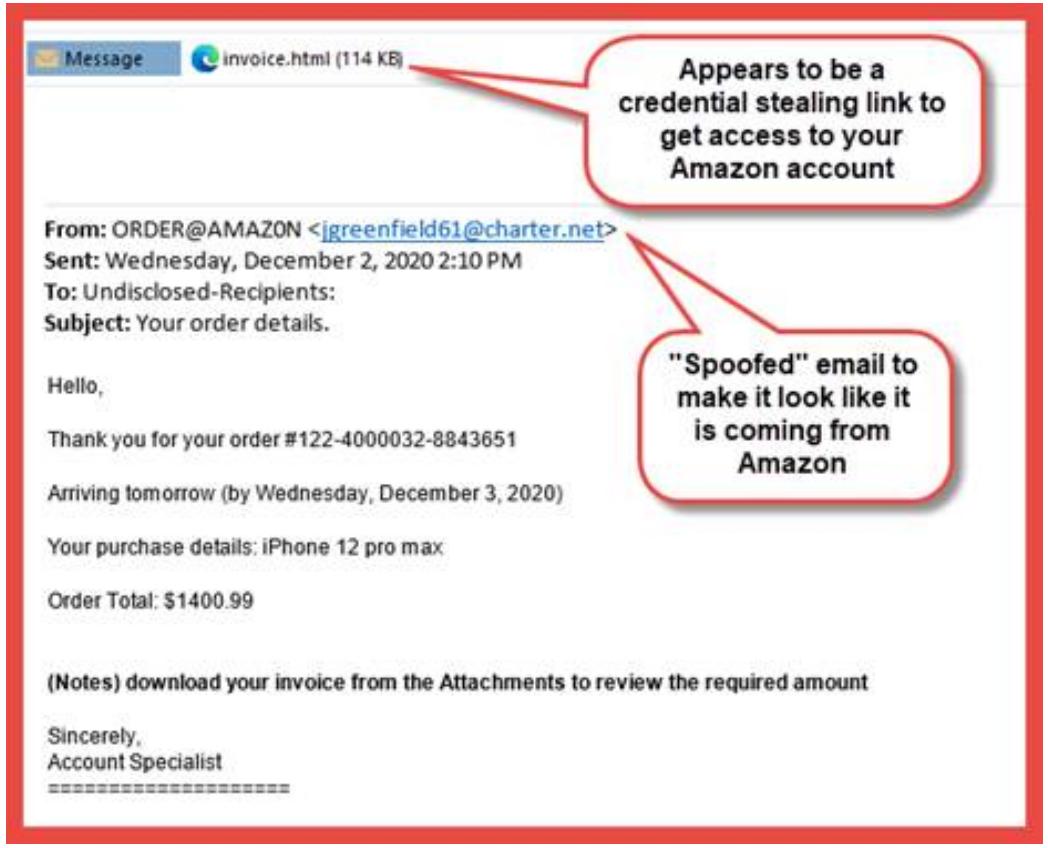
Phishing is the attempt to obtain sensitive information such as usernames, passwords, and credit card details (and, indirectly, money), often for malicious reasons, by disguising as a trustworthy entity in an electronic communication

Phishing scams usually use “Social Engineering” to create a sense of urgency, use coercion, or intimidate someone into responding. They are looking to get your name, login id, and password to hack your account.

- **Fake email from IT requiring you to do something**
- **Fake email pretending that your account will be closed**
- **Fake email pretending to be a trusted vendor (i.e. Amazon, FEDEX, DropBox)**
- **Fake email pretending to be a banking alert**
- **Fake email pretending to be an attorney, HR, IRS, or Social Security**

EMAIL - PHISHING





EMAIL SPOOFING

- Mimics or looks like someone you know, someone you work with, or another trusted party like a vendor or customer
- Typically, it is an “urgent” request for a wire transfer, sensitive information, or some other financial transaction “can you purchase some Amazon Gift Cards”
- Many times the request for something is “confidential” and asks that you do not share this with anyone else

From: Stephen M. Zemaitatis [mailto:maryjoh710@gmail.com]
Sent: Monday, June 15, 2020 12:57 PM
To: Farzetta, John <JFarzetta@riggsdistler.com>
Subject: [EXTERNAL]: REQUEST

Is it safe to say that you are accessible? I need you to address an undertaking for me urgently.

--
Sent from 4G Wireless Phone

EMAIL VIRUSES & MALWARE

Cybercriminals will use embedded links and attachments to spread malicious software

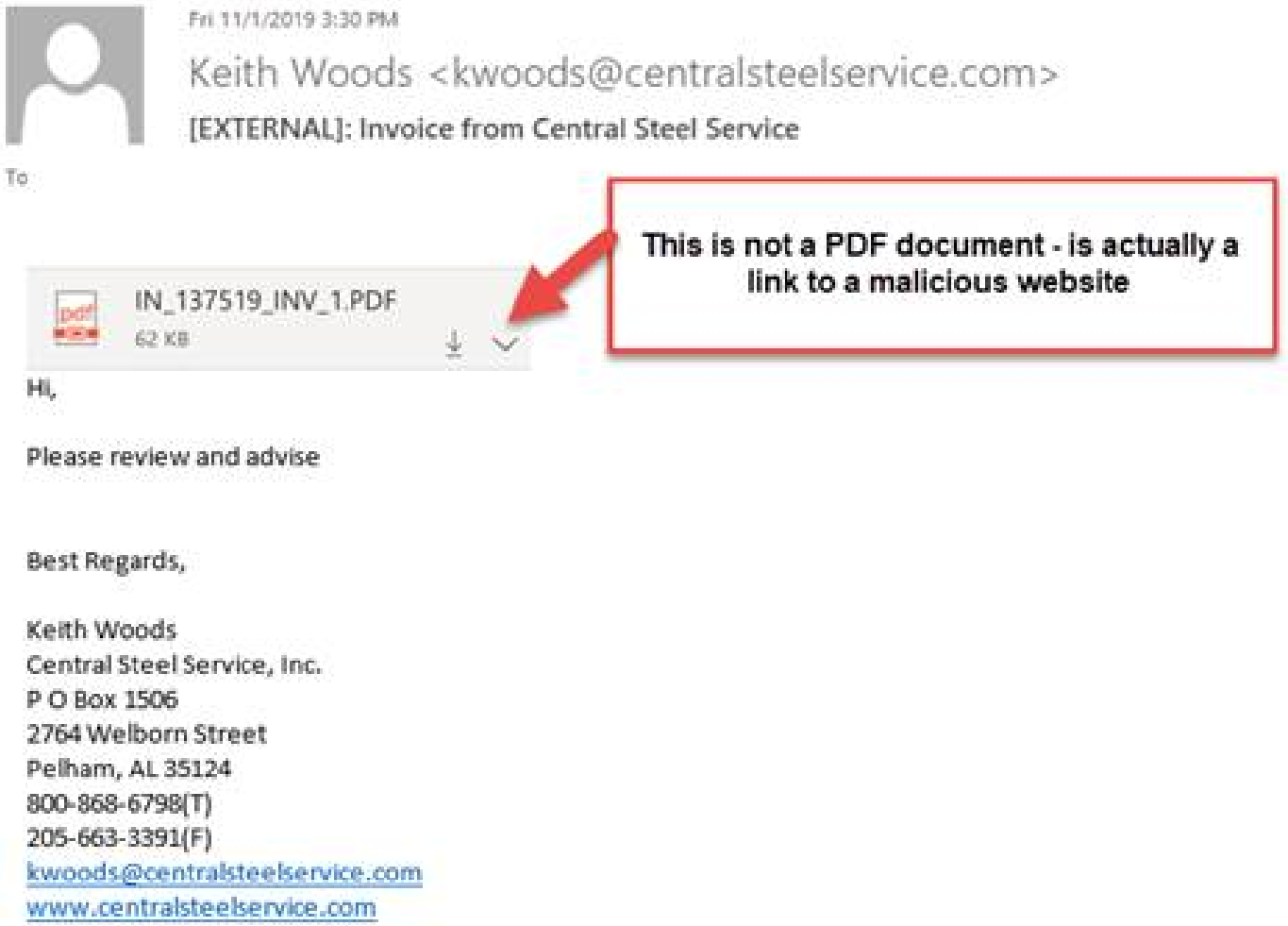
Examples of malware include:

- **Key Loggers – this will track all the key strokes you make and look for patterns that would indicate login id's and passwords**
- **Hijack your webcam or microphone**
- **Re-direct email**
- **Send your data to servers that the hackers control**

What may appear as an attachment, is actually a picture of an attachment with an embedded link behind it

Be aware of any documents sent to you asking to "enable macros" – this can also unleash malware within our systems

EMAIL VIRUSES & MALWARE



RANSOMWARE

- Ransomware is when an attacker either encrypts your data or gains access to the “command & control” functions within an IT organization
- Double extortion – encrypt data and steal it
- They will demand a ransom will typically asked to be paid though a crypto currency as it is virtually untraceable
- Reliable backup processes circumvent this. Riggs Distler has a “3-2-1” backup model and had upgraded it in 2020.
- Average demand: **$850k**, Average paid: **$315k**, YTD 2021 (May 16th) **$81M**
- Examples of ransomware attacks: CNA Financial **$40M;** Colonial Pipeline **$5M**

SOCIAL ENGINEERING

From a Cybersecurity perspective, Social Engineering is the psychological manipulation of people into performing actions or divulging confidential information.

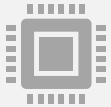
A type of confidence trick for the purpose of information gathering, fraud, or system access, it differs from a traditional "con" in that it is often one of many steps in a more complex fraud scheme.

It has also been defined as "any act that influences a person to take an action that may or may not be in their best interests.“ Usually involves a call to action.

- **IMMEDIATE RESPONSE**
- **CONFIDENTIAL**
- **ACCOUNT DEACTIVATED**
- **LEGAL ACTION**

WIFI - Public

There has been increase in public WIFI. Hackers know this and will mimic what you think may be a secure network (i.e. attwifi) that actually does not exist in the area.



They will also create rogue networks that look like they may be legitimate but are not (i.e. Starbucks Coffee WiFi).

Never use “hidden networks” – once you have joined a hidden network, in the future your pc will look for this hidden network.

Always use VPN into the Riggs Distler network when you are not in a Riggs Distler facility.

CONNECTED SMART DEVICES AND WHAT CAN BE EXPLOITED

Your Smart Phone has become another way in which hackers attempt to gain access to information.

The number of wireless devices has increased dramatically and provides the hackers a wider area to attack.

How do they hack a mobile device

- Downloading malicious apps – hackers will post apps on iTunes and Google Apps that have malicious code
- Clicking on suspicious links – hackers will embed links
- Unsecured public WIFI access

Mobile Device Management (MDM) – controls the apps that can be downloaded, can locate a lost device, can remote wipe a device

MFA (Multi Factor Authentication) & 2FA (Two Factor Authentication)

Multi-Factor Authentication is a method which requires someone logging into a company network is required to provide access authentication to verify their identity in two or more ways.

The verifications are usually a combination of two of the below:

- A password (something you know)
- Receiving a text on your phone (something you have)
- Biometrics: fingerprint, iris of the eye, or facial recognition

PROS – Our customers are asking and requiring it, simplifies login, strengthens security

CONS – Losing a phone – can take a couple of hours to reconfigure

Examples: Amazon, Banks, Empower 401k website

Department of Defense & Customers

CMMC – Cybersecurity Maturity Model

- DoD has aligned a common security framework across all DoD agencies
- Creates a certification process for DoD Supply Chain when handling CUI
- 160 different domain controls
- Level 3 certification by 2025

Customers

- Number of control questions has increased by a factor of four in 5 years
- Cybersecurity standards
- Background check standards
- Physical security standards
- How do we protect their data and what is done when projects are complete