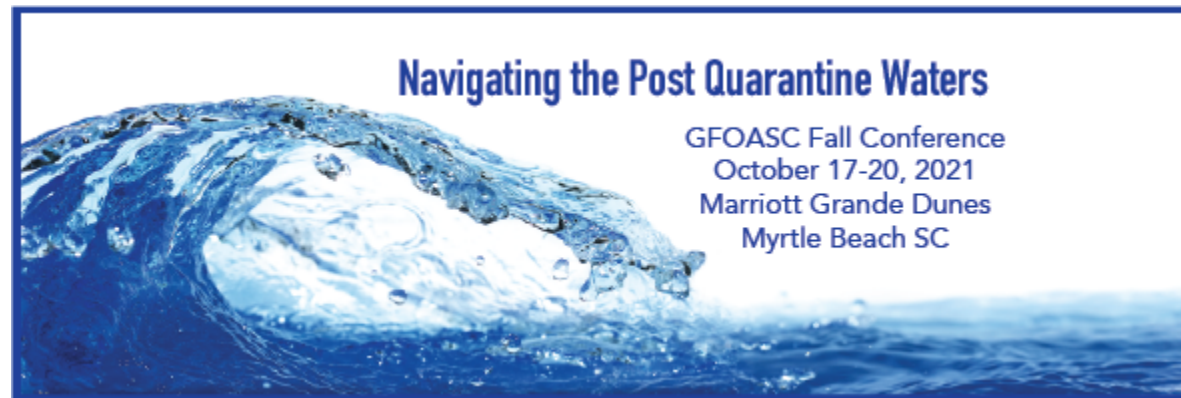


# Updating Your Cyber Security, and Protecting You Against Ransomware Attacks



***Derek Slate, CIC, CSRM***

Surry Insurance  
Vice President of Sales

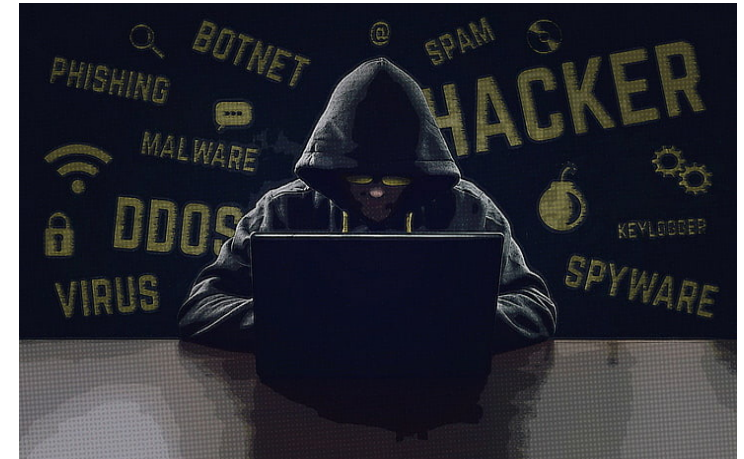


*October 17, 2021*

# Risk

Cyber threats dangers:

- Hackers breaking into systems and altering files
- Viruses erasing the entire systems
- Impostors using your computer to attack others



# Risk

## Intruders stealing confidential information



### **Personally Identifiable Information (PII)**

Most organizations—such as banks, universities and businesses—will never ask for your personal information over the internet

# Risk

- **More About PII**
- PII is information that can be used to uniquely identify, contact or locate a single person



## PII could include:

- Full name
- Address
- Date of birth
- Place of birth
- Driver's license number
- Social security number
- Credit card numbers
- Gender or race

# What can you do?



**If you believe your PII has been compromised these are suggested steps you could take:**

- Change your financial passwords first then change all other passwords
- Remove your computer from the internet if you believe it has been compromised by a malicious code
- Restart your computer in safe mode and perform a full system restore
- Contact financial organizations where you have accounts
- Close or put on hold any accounts that may have been compromised

# Strong Passwords

- "Hackers are using common terms from pop culture and sports to break into accounts online because they know many people are using those easy-to-remember words," said Morgan Slain, CEO of SplashData

## **Not So Good Passwords**

- 123456
- 121212
- qwerty
- 123abc
  - test1
- password
- asdfghjkl

# Think passphrase, not password

- Originally, experts suggested thinking of a super complex password with a variety of numbers, uppercase and lowercase letters, and symbols.
- The problem is they're way too tough to remember. Instead, consider a phrase for your password, then tweak it with numbers or symbols you can more easily recall.

# More Password Tips

- Make them at least 12 characters long. The longer the better
- Uses uppercase and lowercase letters, numbers and special symbols
- Passwords that contain of mixed characters are harder to crack
- Don't use memorable keyboard paths
- Don't use your personal information
- Password should be unique for each account you have



# The Most Dangerous Web's Search Terms

Search



- A study by McAfee, Inc., an internet security company, exposed the riskiest searches one can perform on common search engines such as Google
- McAfee searched 2,658 popular keywords and phrases across 413,368 URLs to analyze the risk percentage of certain terms

# The Most Dangerous Web's Search Terms

## McAfee, Inc. Study

- The study considered the search term **“screensavers”** as the most dangerous keyword to use in search engines, it returned a maximum risk of 59 percent



# The Most Dangerous Web's Search Terms

## McAfee, Inc. Study

- Entering the word **“lyrics”** in any phrase in a public search engine returns one risky site for every two search results

### Nobody Knows the Trouble I've Seen

African American Spiritual

musical score for the African American spiritual "Nobody Knows the Trouble I've Seen". The score is written in 4/4 time and consists of three staves of music. The lyrics are: "No-bod - y knows the troub-le I've seen, No-bod - y knows my sor-row, No-bod - y knows the troub-le I've seen, Glo - ry hal - le - lu - jah 1. Some-times I'm up, some-times I'm down, Oh yes, Lord, Some times I'm al-most to the ground, Oh yes, Lord. 2. Oh, don't you see me going to slow, Oh yes, Lord. I have my troubles here below, Oh, yes Lord. Refrain". The source is cited as bethsnotes.com.

# The Most Dangerous Web's Search Terms

## McAfee, Inc. Study

- Employees who clicks on a search engine result that contains the word “**free**” has nearly a 22 percent chance of infecting your computers with threatening material like spyware, spam, adware, viruses or other malware



# Those Annoying Cookies

## So what a Cookies

- When you visit a webpage, a cookie is placed on your computer as a unique identifier
- Cookies allow a web server to store information on your computer and later retrieve it—like a personalized user ID





# Cookies

- Cookies have many useful capabilities
  - They allow the customization of website experiences and let e-commerce businesses track visitors, page hits and popular pages
  - Internet settings can be personalized for higher or lower security levels regarding cookies



# Ransomware

- Ransomware attacks which entail a cybercriminal deploying malicious software to compromise a device (or multiple devices) and demand a large payment be made before restoring the technology



# The Surge of Ransomware Attacks

The recent debut of Ransomware-as-a-Service (RaaS)

- RaaS refers to a dark web business model that permits sophisticated cybercriminals to sell their ransomware software to willing buyers (usually less skilled cybercriminals), who then utilize the software to launch an attack and secure a ransom payment

• Well-known RaaS incidents include

- WannaCry
- Cerber
- MacRansom
- Philadelphia
- Atom
- Hostman
- FLUX





# Best Practices for Combatting Ransomware Attacks


## Secure your systems by:

- Using a virtual private network (VPN) for all internet-based activities
- Installing antivirus software
- Implementing a firewall to block cybercriminals from accessing your organization's VPN
- Restricting employees' access to websites that aren't secure



# Best Practices for Combatting Ransomware Attacks

## Secure your systems by:

- Establishing email filters to keep phishing messages from reaching employees' inboxes
- Encrypting sensitive data on all organizational devices and routinely backing up this information 
- Limiting which employees receive administrative controls to prevent inexperienced staff from mistakenly downloading a malicious program

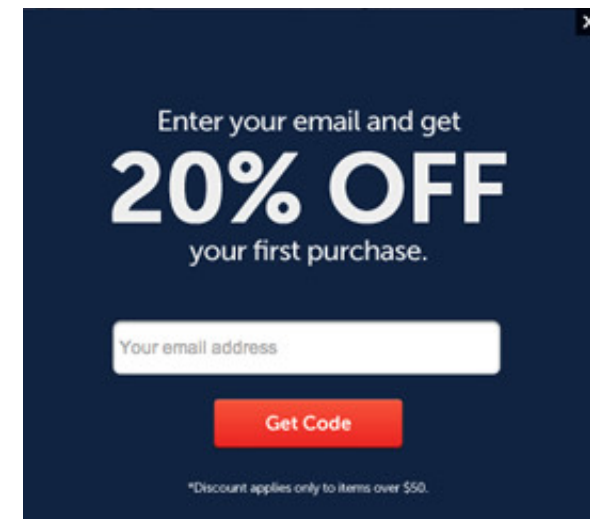


# Best Practices for Combatting Ransomware Attacks

Train employees on how to prevent and respond to a



- Avoid opening or responding to emails from individuals or organizations you don't know
- Never click on suspicious links or pop-ups—whether they're in an email or on a website




# Best Practices for Combatting Ransomware Attacks

- Only browse safe and secure websites on organizational devices
- Refrain from using workplace devices for personal browsing
- If you suspect a ransomware attack, report it to the IT department immediately



# Multi-Factor Authentication (MFA)

- Multi-factor authentication  refers to the use of two or more means of identification and access control—sometimes referred to as
- Something you have
- Something you know
- Something you are



# Multi-Factor Authentication (MFA)

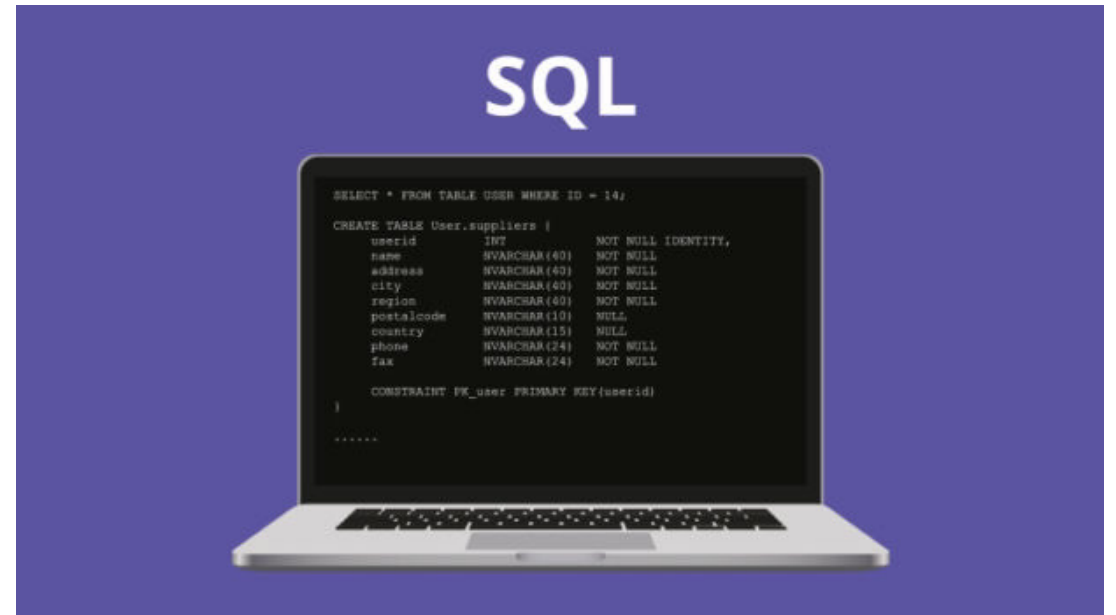
- A username and password, for example, is something you know
- Requiring a code sent via text message (SMS) establishes “something you have,” i.e., a mobile phone belonging to you
- Biometric authentication, through a fingerprint or retina scan, establishes “something you are”

**It**   
**takes**  
 **two**

# Most Common Cyber Attacks

## SQL injection

- An SQL (structured language query) injection attack is a type of cyber-attack used to take control of the system and steal data from a database or to bypass the logins





# Most Common Cyber Attacks

## Phishing

- It is when cybercriminals target victims by email attachments or messages that appear to be from a legitimate company asking for private information
- Phishing attacks are often used to fool citizens into giving over credit card data and other personal information





# Phishing Loss Trends

- A new organization fell victim to ransomware every **two minutes** in early 2016, every **14 seconds** in 2019, and projected will be every **11 seconds** in 2021

(Source: Cyber Security Ventures)

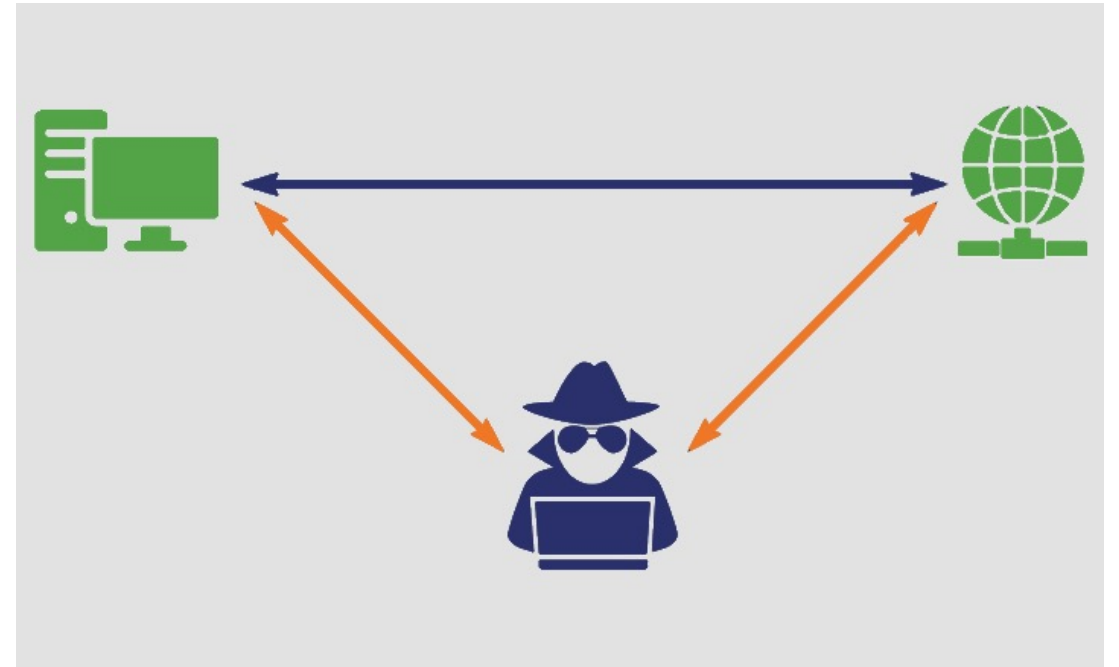


- **1.5 million** new phishing sites are created **every month** and ransomware attacks coming from phishing emails increased **109 percent from 2017 to 2019** (Source: webroot.com and PhishMe)

# Most Common Cyber Attacks

## Man-in-the-middle attack

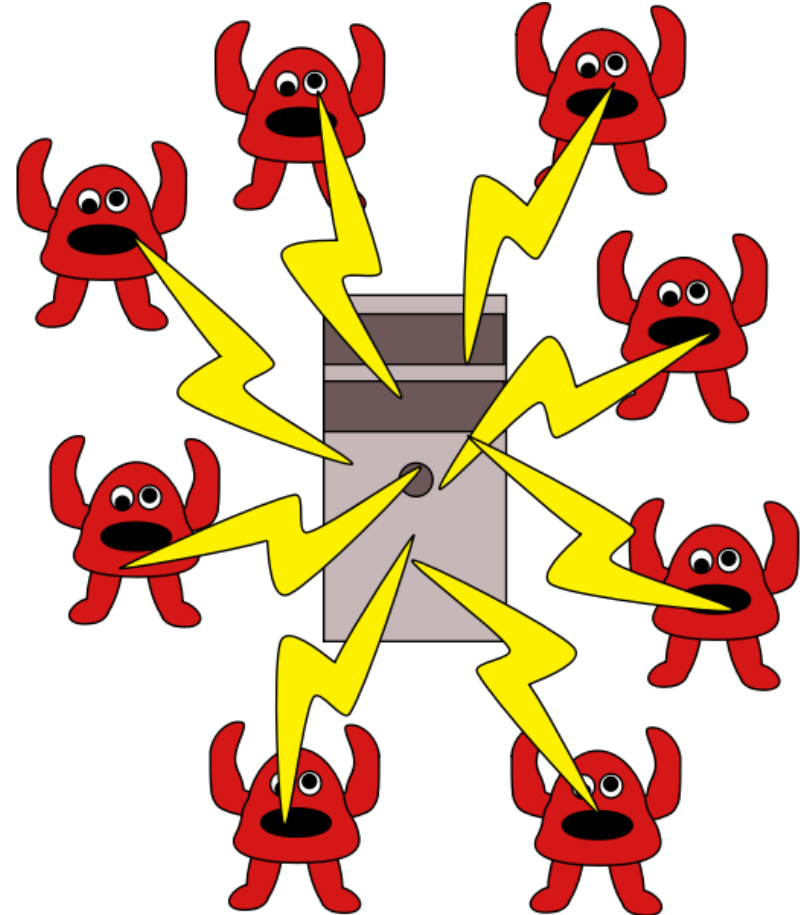
- M.I.T.M attacks are simple types of digital attacks where a cybercriminal intercepts communication between two routers or towers in order to leak data
- For example, on an open WiFi network connection, an attacker can sniff data being passed from the victim's device and the router




# Most Common Cyber Attacks

## Denial-of-service attack

- A denial-of-service attack is an attack where cyber hackers protect a computer system from giving legitimate requests by overloading the networks and servers with unwanted and fake traffic
- This makes the network and system unusable, preventing a company from carrying out vital functions



# Cyber Risk Management

- If your organization stores data and information digitally, you should have a cyber-risk management program that:
- Addresses prevention 
- Disclosure
- Crisis management
- Insurance coverage in the event of a data breach

Cyber risk management requires the planning and execution of all 4 of these components:

# 1-Develop Strategies to Prevent a Data Breach

- Your data breach prevention strategies may include encrypting all devices used by your employees, such as laptops, tablets and smartphones
- Encrypting these devices will prevent unauthorized access if a device is lost or stolen



## 2-Know Your Disclosure Responsibilities

- If you experience a data breach, you may be legally required to notify certain people



# 3- Have a Crisis Management and Response Plan

- Preparedness is key when developing your cyber risk management program
- When you experience a data breach, you need to be prepared to respond quickly and appropriately
- This is where your crisis management and response plan come into play



# 4- Protect Your Data—and Your Organization

- Your cyber risk management program should include cyber liability insurance coverage that fits the needs of your organization
- Cyber liability insurance is specifically designed to address the risks that come with using modern technology—risks that other types of business liability coverage simply won't cover





*Learn from the mistakes of others.  
You can't live long enough to make  
them all yourself.*

— Eleanor Roosevelt

*Once inside a network, attackers maximize the amount of damage by encrypting as much data as possible. Their objective is to compromise a victim's network so extensively it cannot recover, forcing the victim into a payment scenario.*

— Kevin Haley, Symantec Security Response

## **Sources and Additional Reading**

1. SonicWall, “2020 Cyber Threat Report.”
2. Coveware, “Ransomware Costs Double in Q4 as Ryuk, Sodinokibi Proliferate.”
3. U.S. Gov’t, “How to Protect Your Networks from Ransomware.”
4. Accenture, “Managing Ransomware: Practical Steps to Avoid Future Attacks.”

Thank You for  
attending this  
session