# CYBERSECURITY AWARENESS

Agenda:

- Introductions
- Current Local Trends
- Common Types of Cyber Attacks
- Best Practices
- Resources
- Questions

Encinitas
CHAMBER OF COMMERCE

# Presenters

Captain Lawrence

San Diego Sheriff City of Encinitas

Jessica Contreras
City of Encinitas IT Director
Infragard SD Cyber Council

Darren Bennett
Former FBI Cyber / San Diego CISO
Infragard SD Cyber Council

Cameron Matthews
Nth Generation
Virtual CISO

# Introduction to Cybersecurity

Cybersecurity is the process of protecting your digital information and computer systems from cybercriminals.

- Cybercrime can impact all businesses and organizations regardless of size
- The average cost of recovering from a cyber incident was over $1.8M in 2022 (Forbes)
- Cybersecurity awareness and implementation of best practices can help protect your organization

# State of Cybercrime

National Trends:

In 2022, over 800,000 complaints were received by the FBI’s Internet Crime Complaint Center (IC3).  This is a 5% decrease from 2021.  However, the total loss as grown from $6.9 billion in 2021 to more than $10.2 billion in 2022.

Ransomware continues to be the #1 threat which is facilitated by phishing attempts.

Phishing attempts are increasing with the use of ChatGPT

Supply chain attacks are a major concern - SolarWinds Attack has over 30,000 victim organizations to date

**Data Breaches - average cost of remediation is $4.5 million**

Cloud Security Misconfiguration is a growing trend - If you store your data in the Cloud, you may still be responsible for its security

Cryptojacking has decreased recently due to the devaluing of cryptocurrencies.
San Diego County alone lost $80 million in 2022

Threats from Nation State Actors is on the rise - Russian, North Korean, Iranian and Chinese - affiliated groups are using ransomware to fund war, nuclear programs and gather intelligence.

San Diego Trends:
Non-payment/non-delivery scam is #1 - over 28,000 instances in 2022
Personal Data Breach - over 8,000 instances
Investment impersonation scam - over 4,900 instances
Extortion (Ransomware) - 4,700 instances
Tech Support - 4,400 instances

Keep your systems up to date!  Validate and Verify!

# Common Types of Cyber Attacks

## Phishing

A social engineering scam where the hacker lures the victim to provide information such as account numbers or passwords. They may pose as a coworker or friend using email, phone, or text.

## Ransomware

Ransomware is a type of malicious code (malware) designed to encrypt files. The cyber actors then request ransom to restore the files.
Ransomware can be delivered in an email, text message, or by clicking a malicious link.

## Email Compromise

Business email compromise occurs when a hacker takes control of someone elses email account. They are then able to read emails and often spread malware using the compromised address book.

## EFT Fraud

Electronic Funds Transfer Fraud occurs when a fraudster posing as someone else such as a vendor redirects payments to their accounts. They may use business email compromise to intercept emails from a business for this purpose.

## Network hacker attack

This would typically occur to a business's:

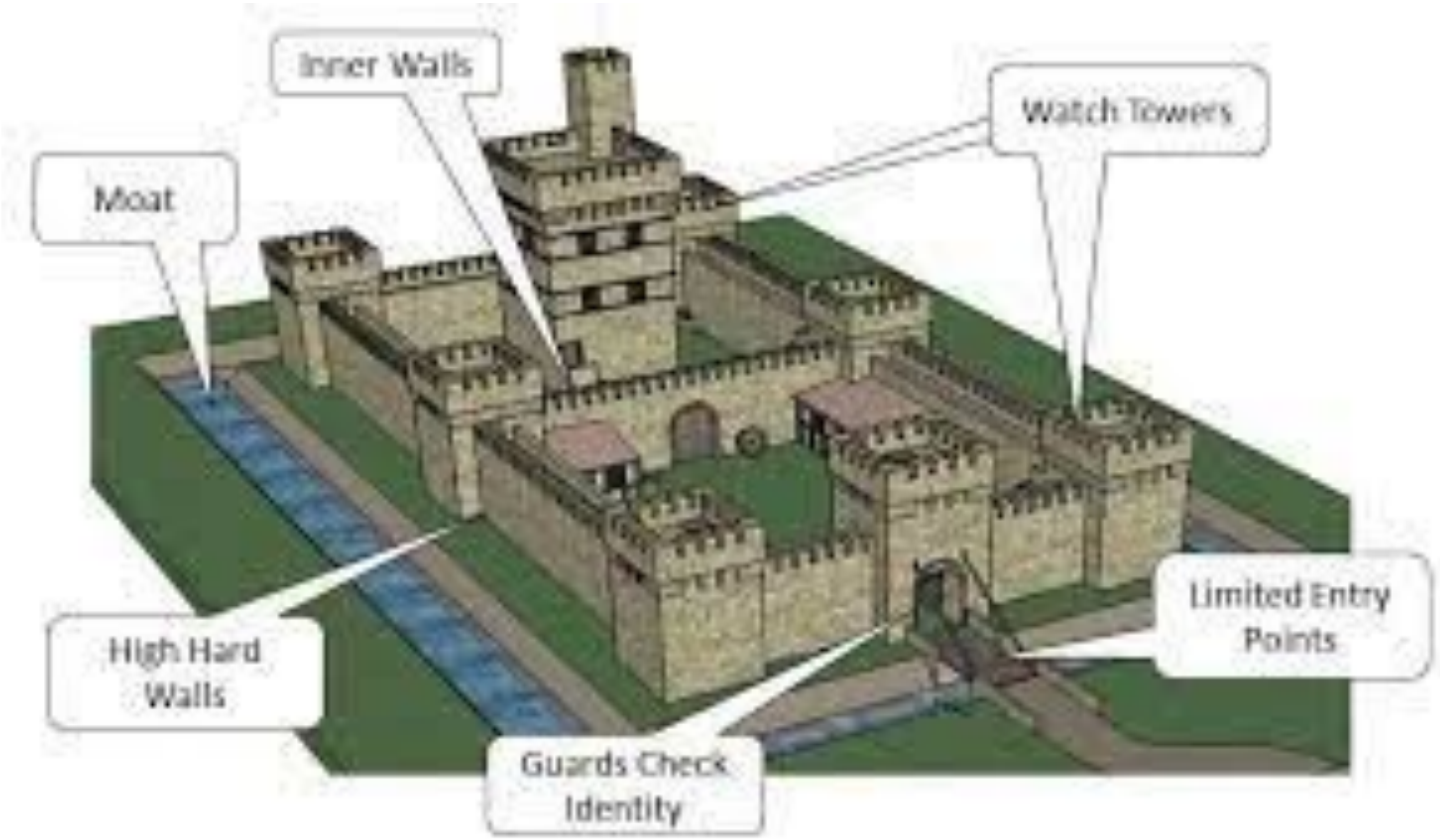
- marketing website
- employee/partner portal
- e-commerce website

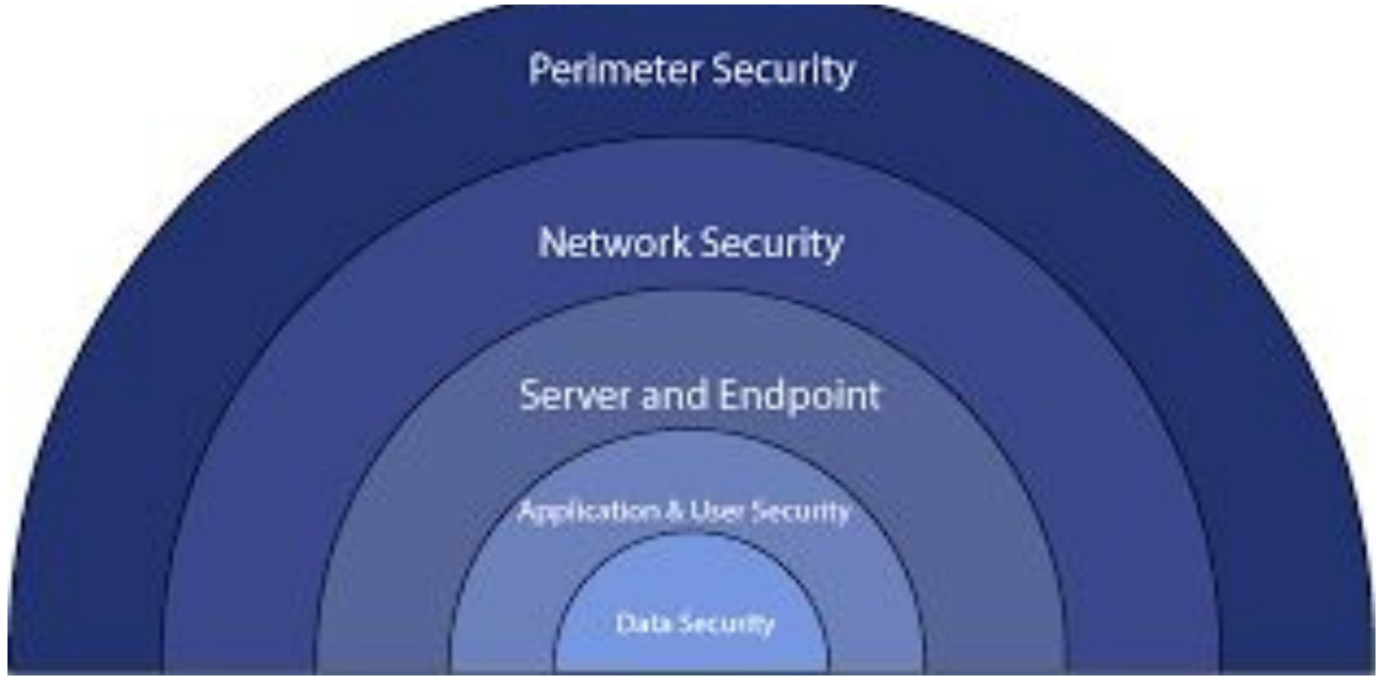
The main security issues are:

- services missing patches
- application misconfigurations

# Cyber Security Best Practices

- Security is a **<u>layered approach</u>**
  - There is no “Silver Bullet”
  - Like any security system, there needs to be multiple means of protection (Think Castle)
  - This briefing is a good start, but NOT all inclusive…





# Cyber Security Best Practices

- **For more detailed security guidance:**
  **Use a security framework***
  - CIS 18 Critical Controls
    https://www.cisecurity.org/controls/cis-controls-list
  - NIST 800-53
    https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf
  - NSA Best practices for security home networks
    https://media.defense.gov/2023/Feb/22/2003165170/-1/-1/0/CSI_BEST_PRACTICES_FOR_SECURING_YOUR_HOME_NETWORK.PDF

*These assume a surprisingly high level of understanding of cyber and IT. If needed, ask your IT expert for help!

CIS Center for Internet Security®
Creating Confidence in the Connected World.™

NIST
800-53
Revision 5
Security Controls

NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA
CYBERSECURITY

# Cyber Security Best Practices

- Best practices - Overview:
    - Have a plan (Incident Response Plan) - If you don’t have a plan on where you are going…
    - Identify who is responsible for security and have a backup person as well
    - Create a contact list: Know who in your organization to work with (Executive team, Legal, RISK, IT) and when. Other important entities:
        - Law Enforcement coordination center - for reporting and incident assistance, IC3.gov (FBI reporting)
        - Key Vendors contacts and phone #s
        - MSP (Managed Security Provider) - A contracted security provider monitoring your systems
    - Buy cyber insurance
    - Use a managed security provider (MSP) - if you can
    - Know which systems are most important to your organization and what is in place to protect them!
    - Educate your users (online training is available, some for free)
    - Keep systems patched, use multi-factor authentication, ensure you have firewalls, anti-virus, endpoint security and other security software in place and monitored
    - “Think before you click”
    - **Have good backups and TEST them**

**<u>We will explain some best practices in the following slides:</u>**

# Complex Passwords

The longer a password is, the harder it is to crack.  A current length of 12 characters or greater is recommended.  The password should contain:

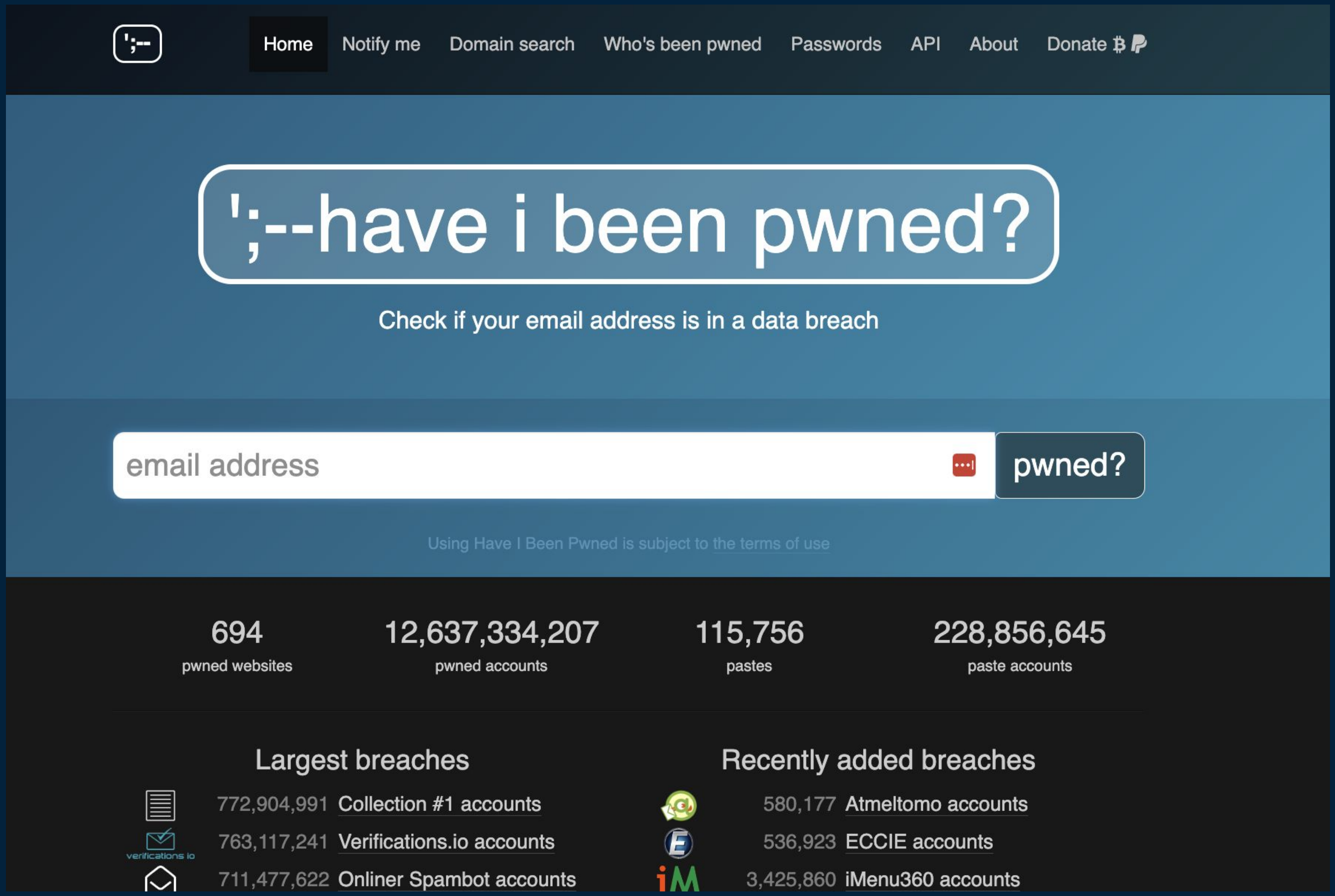
- a combination of special characters
- numbers
- upper-case
- lower-case letters

@fterTheB3@chW33@tBurritos

# Multi Factor Authentication (MFA)

*MFA requires a minimum of two pieces of information to access a system such as a password and a code texted to your phone.*

Multi-Factor Authentication (MFA)
user login
*********
Allow access?
YES
WELCOME



';--have i been pwned?

Check if your email address is in a data breach

Using Have I Been Pwned is subject to the terms of use

694 pwned websites

12,637,334,207 pwned accounts

115,756 pastes

228,856,645 paste accounts

Largest breaches

| | |
|---|---|
| 772,904,991 | Collection #1 accounts |
| 763,117,241 | Verifications.io accounts |
| 711,477,622 | Onliner Spambot accounts |

Recently added breaches

| | |
|---|---|
| 580,177 | Atmeltomo accounts |
| 536,923 | ECCIE accounts |
| 3,425,860 | iMenu360 accounts |

- What about just complex passwords? (haveibeenpwned.com)
- MFA/2FA - Effective means of protecting your access
- REQUIRED for effective security

# Inventory

Maintain an inventory listing the hardware and software your business or organization uses including:

- Vendor Name
- Vendor Contact Information
- Make/Model
- Version

An inventory is useful for keeping informed regarding patches and security bulletins related to your computer assets.  It is also useful if you are breached to receive customer support assistance.

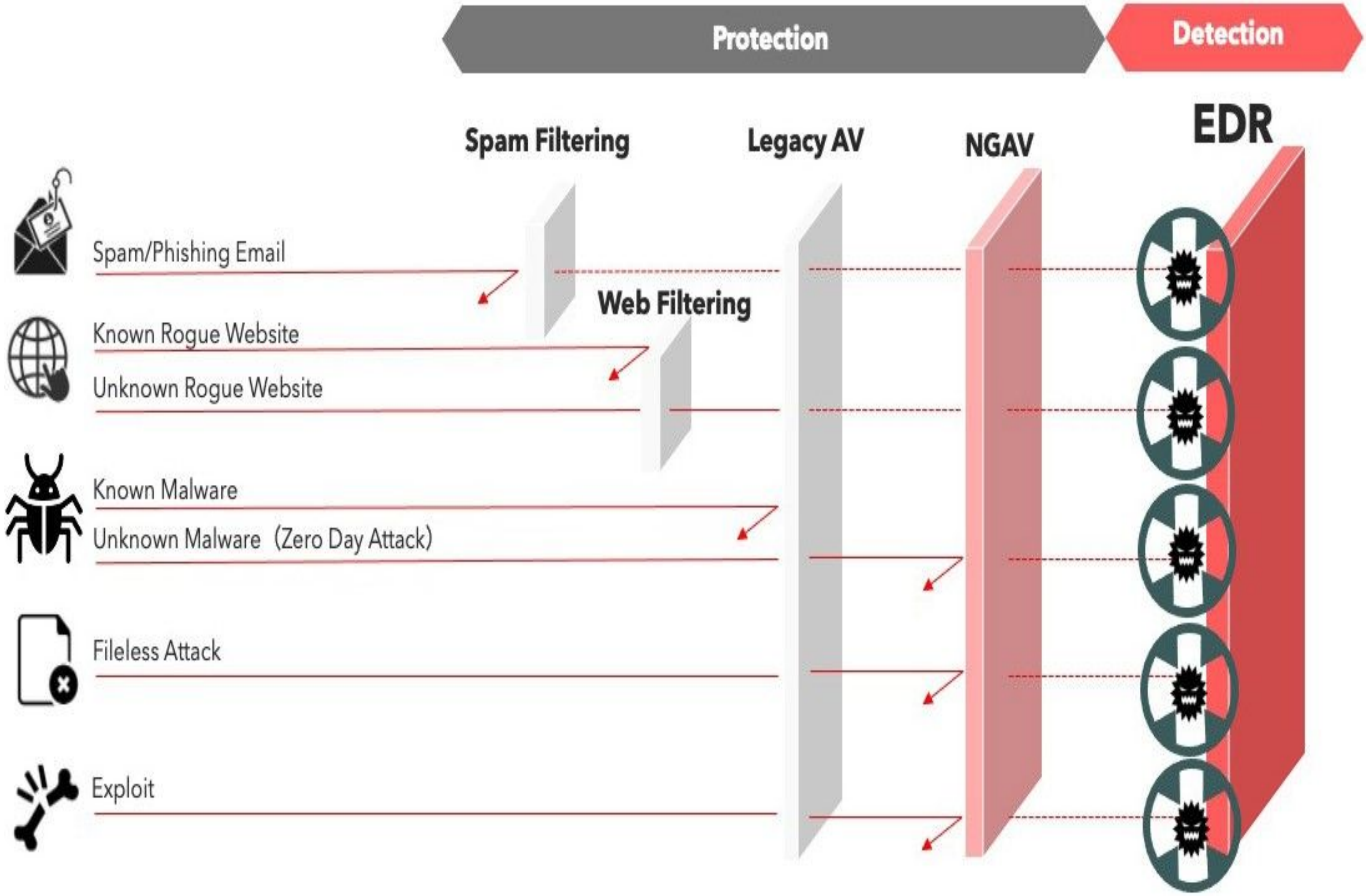
# Patching Devices

*Patching is the process of installing software updates to keep your systems secure.*

- Most basic line of defense
- ALL organizations struggle
- While with the FBI, 100’s of incidents.. 90% could have been prevented with proper patching
- Patch everything.. not just Operating System. Don’t forget your applications

# Anti-virus/End Point Detection Response

- Is Antivirus enough? “Depends” (probably not)
- Favorite part of a layered defense approach is End Point Detection and Response (EDR)...
- If malicious content gets past all the other layers, this is the last line of defense.
- Ransomware example.. EDR can stop the encryption before it occurs and alert IT.



# Email Filtering

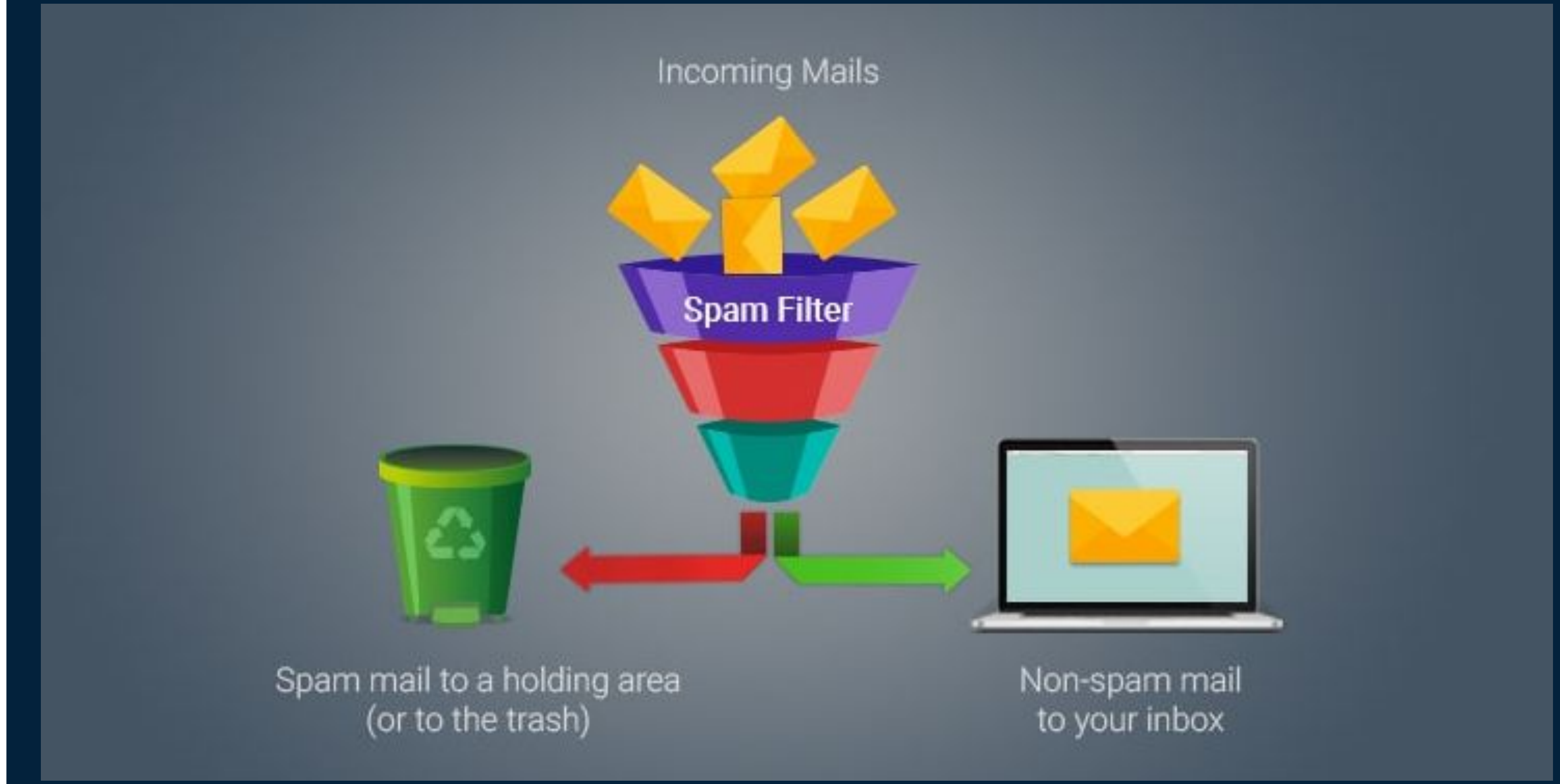
Email and file filtering check emails and attachments for malicious code and quarantine these files before the user receives them in their email box.  A “sandbox” may be included where attachments are opened and analyzed before a user receives them.

Examples include:

Microsoft Defender

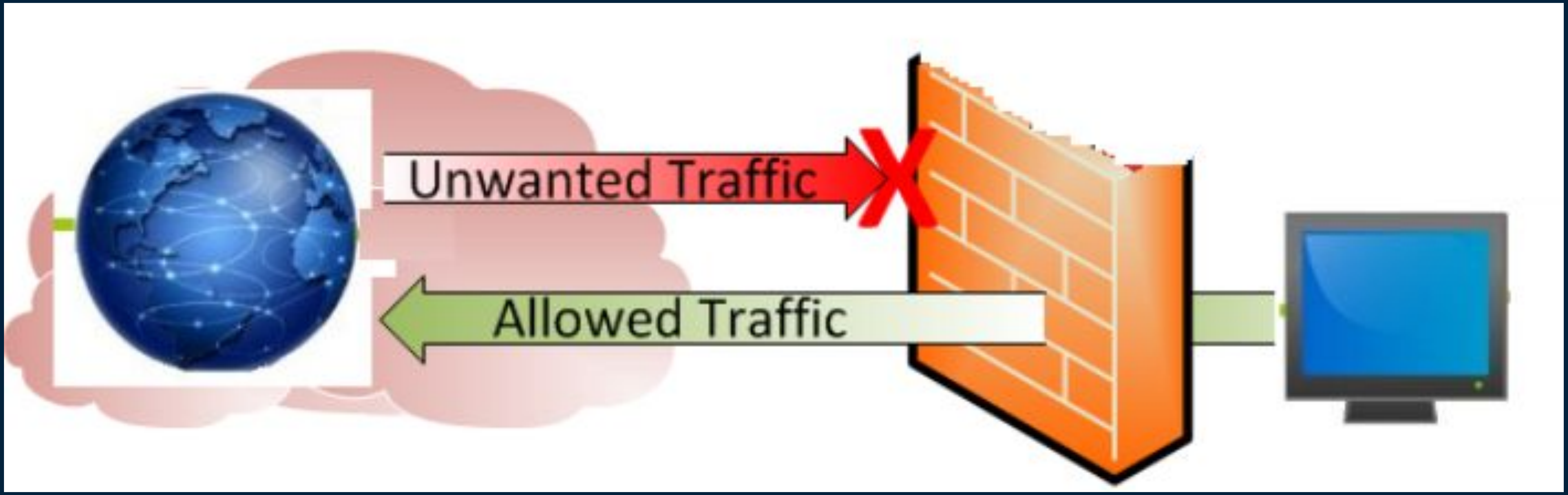
Avanan

GMail Spam Filter



# Firewall

A firewall acts as a security guard for your network allowing certain traffic identified by IP Addresses to access your network while blocking other traffic. Firewalls can be configured to receive updated lists of malicious IP Addresses to block.

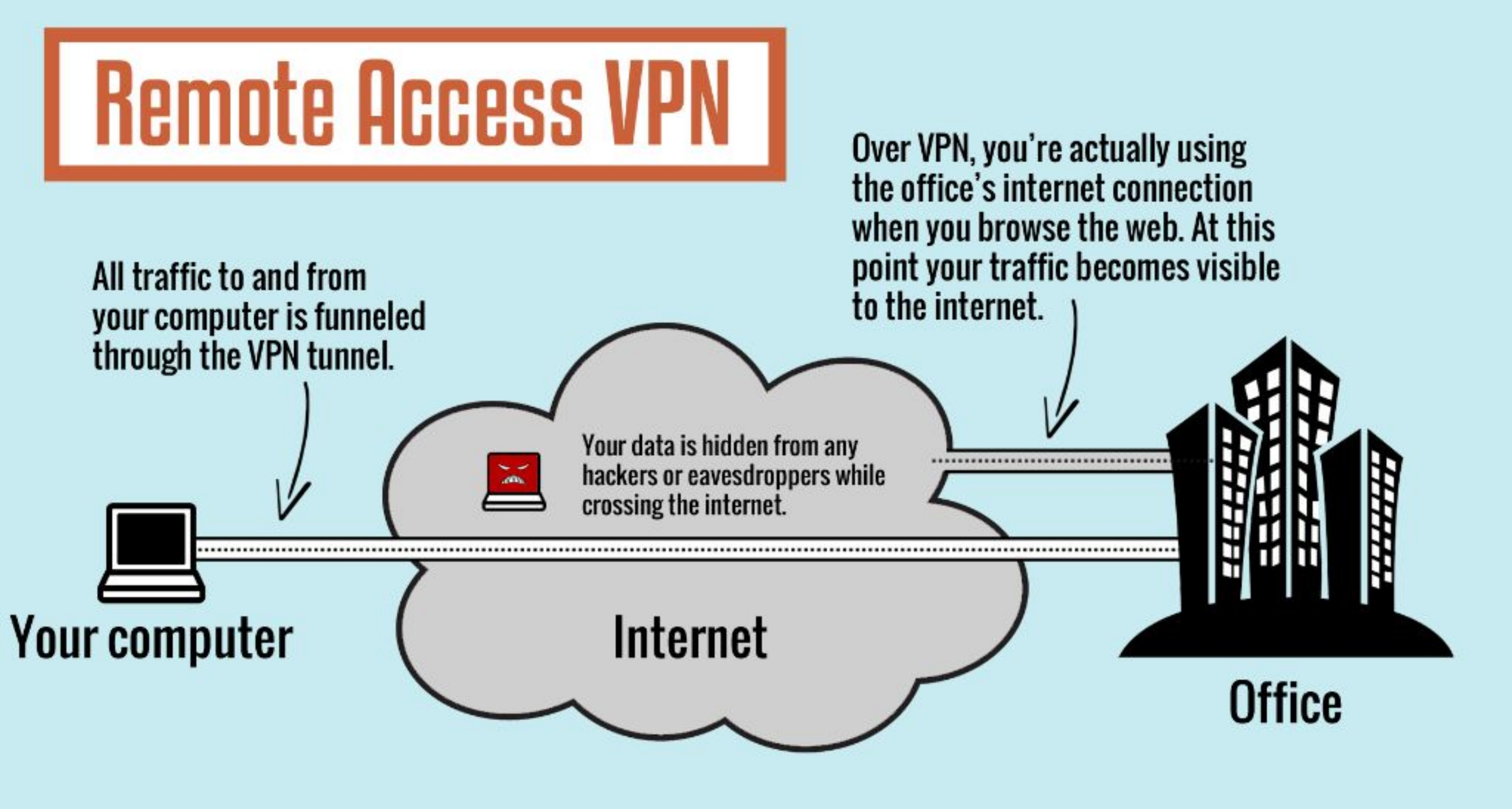


# Geofencing

- Geofencing is when an organization creates virtual boundaries around specific locations or zones
- For example, only allowing access from specific counties
- This is done via software and/or hardware at various levels including your firewall, email systems and more
- Increasingly common

# Virtual Private Network (VPN)

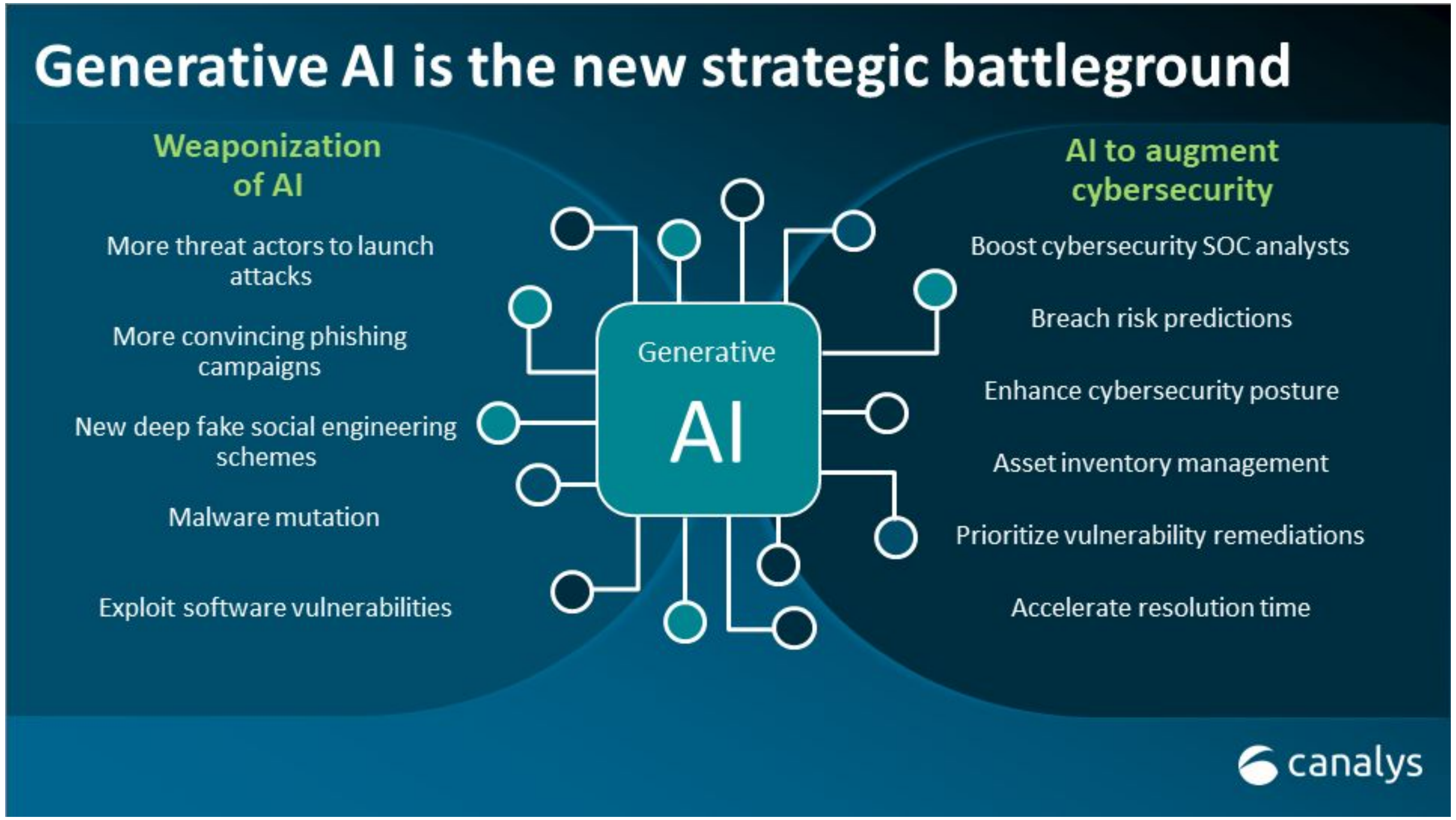
*A VPN encrypts (scrambles) data that is passed over a network to make it illegible if it is intercepted by a hacker. This is useful for protecting confidential information while it is in transit such as intellectual property, bank account information, and network credentials.*



Remote Access VPN
All traffic to and from your computer is funneled through the VPN tunnel.
Over VPN, you're actually using the office's internet connection when you browse the web. At this point your traffic becomes visible to the internet.
Your data is hidden from any hackers or eavesdroppers while crossing the internet.
Your computer
Internet
Office

# Be cautious when using AI

- What is AI?
- AI is a double edged sword
- It is VERY difficult (if not impossible) to get back sensitive information once entered into ChatGPT/Google Bard
- Need governance and policies in place
- Users need guidance on what is ok to share with AI systems and what is not. Checkout AI policy frameworks shared online - Google “AI policy examples”



## Generative AI is the new strategic battleground

**Weaponization of AI**

- More threat actors to launch attacks
- More convincing phishing campaigns
- New deep fake social engineering schemes
- Malware mutation
- Exploit software vulnerabilities

**AI to augment cybersecurity**

- Boost cybersecurity SOC analysts
- Breach risk predictions
- Enhance cybersecurity posture
- Asset inventory management
- Prioritize vulnerability remediations
- Accelerate resolution time

canalys

# Training

*The methods that will most effectively minimize the ability of intruders to compromise information security are comprehensive user training and education.* – Kevin Mitnick

- Make sure to train yourself & your staff on these best practices!
- Encinitas Chamber of Commerce Learning Workshops
- CISA | StopRansomware.gov
- San Diego Cyber Lab
- Local Colleges

# Cybersecurity Resources

**CISA** **www.cisa.gov**

https://www.cisa.gov/cyber-guidance-small-businesses

Action plan for small and medium sized businesses to create a secure environment and security culture within their companies.

https://www.cisa.gov/audiences/small-and-medium-businesses

Free tools and information that will help get your business into what we call a more secure cyber posture.

https://www.cisa.gov/about/regions/region-9

CISA Region 9 (California, Hawaii, etc) regional cybersecurity information

**StopRansomware.gov**

one stop location for tools and resources to combat ransomware

**IC3 (Internet Crime Complaint Center)** **www.ic3.gov**

FBI's platform for reporting cybercrime

**San Diego Regional Cyber Lab** **www.sandiego.gov/cyber-lab**

Cyber information, training, tools, and virtual and physical lab facilities to learn and sharpen your cyber skills

**Encinitas Chamber of Commerce Cybersecurity Resources Guide** **https://encinitaschamber.com/cyber-security/**

Free webinars, links to resources, compact and comprehensive starting line to help small businesses build a cyber program

# Who should I contact if breached?

Cyber Insurance Provider

IC3 Internet Crime Complaint Center (www.ic3.gov)

San Diego Law Enforcement Coordination Center

SD Sheriff Non Emergency (North County)

# Q & A

Encinitas
CHAMBER OF COMMERCE