MERS®
Municipal Employees' Retirement System

Cybersecurity Threat Landscape: What's New, What's Coming

Scott Thompson, MERS Cybersecurity & Facilities Director

September 2023

Agenda

Where Are We Today?

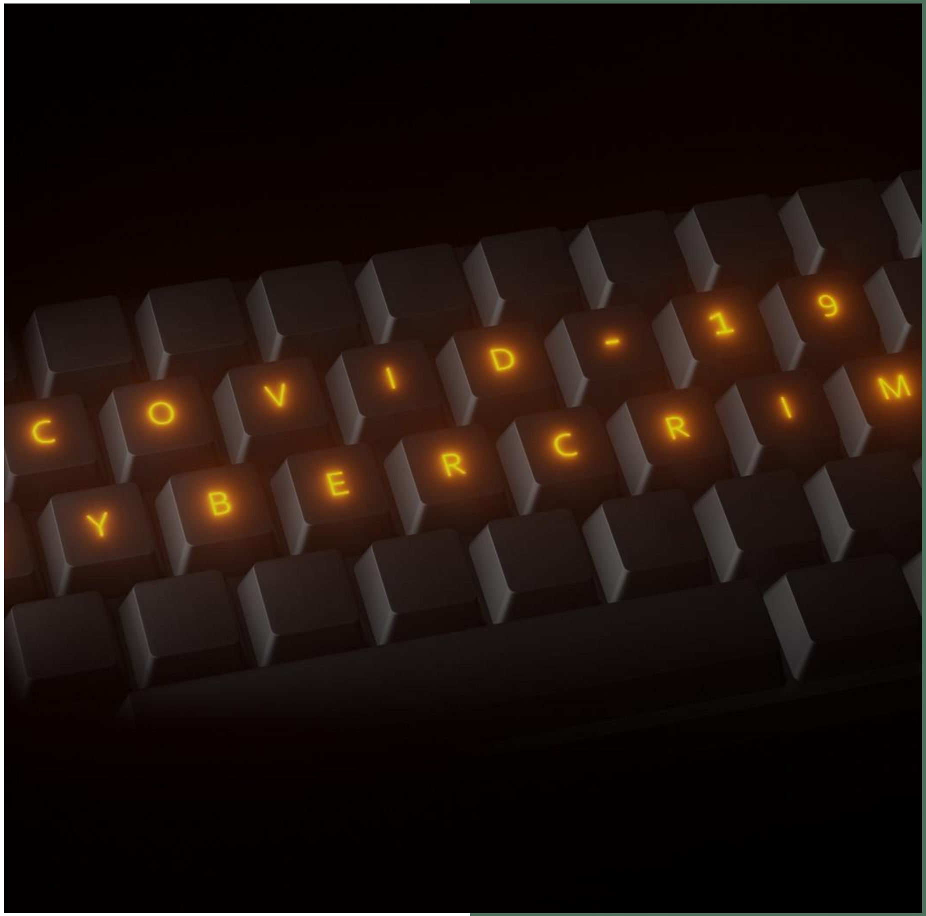
- Pandemic’s Impact on Cybersecurity
- Cyber Crime’s Impact on Organizations
- Social Engineering Attack Tactics
- Protecting Yourself and Your Family
- MERS’ Cybersecurity Practices

What’s What’s Coming?

- “Passwordless” Environments
- Internet of Things (IoT)
- Artificial Intelligence (AI)

MERS®
Municipal Employees’ Retirement System

Pandemic's Impact on Cybersecurity



MERS®
Municipal Employees' Retirement System

Effects of the Pandemic on Cybersecurity

Cybercrime has risen by **300%** since the pandemic began

- Emotional turmoil
- Inexperience with remote work connectivity
- Vulnerabilities of remote work processes

Remote workers are **more likely** to fall for a cybercrime through their work email

- A State, Local, Tribal, and Territorial (SLTT) assessment last year by the Cybersecurity and Infrastructure Security Agency (CISA) revealed a click rate of **nearly 14%**

MERS®
Municipal Employees' Retirement System

Source: knowbe4.com

In March 2022, the FBI issued a stark warning to local U.S. governments and public services:

"Ransomware attacks against regional and local governments were disrupting operational services, posing risks to public safety, and generating financial losses." The impact of these attacks, it said, are "especially significant due to the public's dependency on critical utilities, emergency services, educational facilities, and other services overseen by local governments."

Within the government sector, **local government entities** had become the second highest victimized group behind academia.

Source: knowbe4.com

MERS®
Municipal Employees' Retirement System

Root causes of attacks in state and local government

- Exploited vulnerabilities (38%)
- Compromised credentials (30%)
- Email-based attacks - malicious emails or phishing (25%)

Source: sophos.com

Cyber Crime's Impact on Organizations

MERS
Municipal Employees' Retirement System

Did You Know?

! On average, it takes 206 days to discover a **data hack** and the average company incurs approximately $4.5 million per incident. (down from 274 days!)

Protection Measure: 365 On-Demand Vulnerability Scanning

! 1.7 million **ransomware** attacks occur daily and average $1.9 million per incident.

Protection Measure: Ransomware Simulation

! 75% of breaches involve **human error** by employees.

Protection Measure: Social Engineering Evaluation

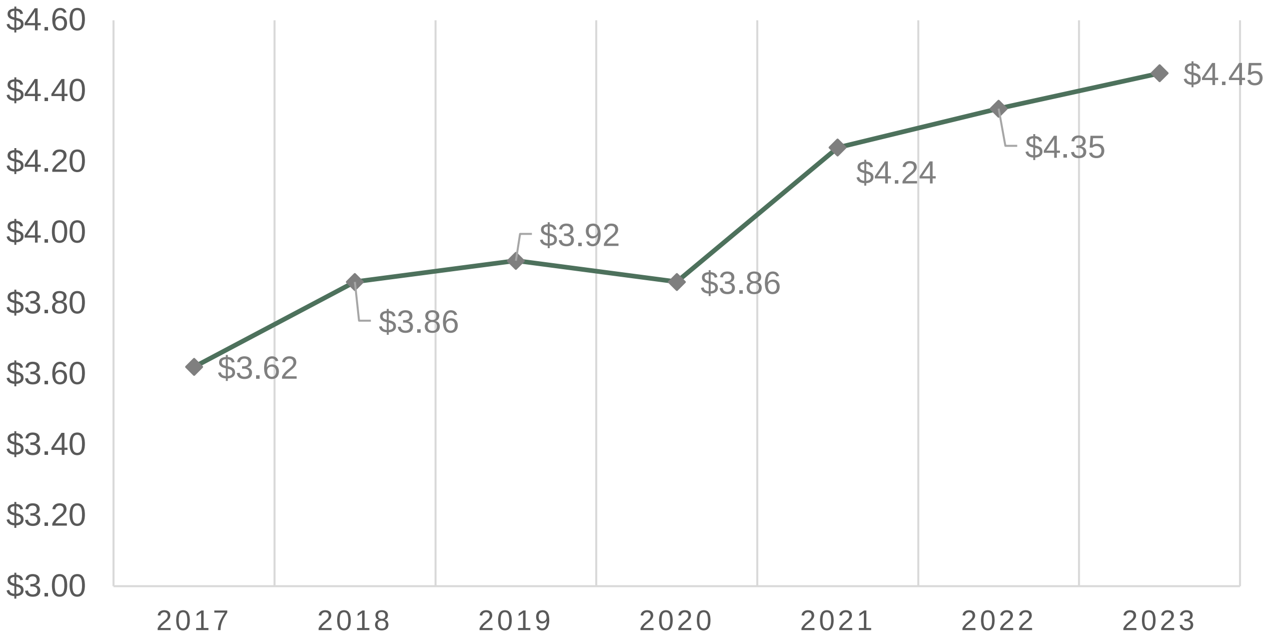
! 80% of 2022 breaches were caused by **3rd party vendors**.

Protection Measure: Vendor Management Risk Assessment

Source: ibm.com

Worldwide Breach Costs - 2023

Average total cost of a breach by year (in millions)



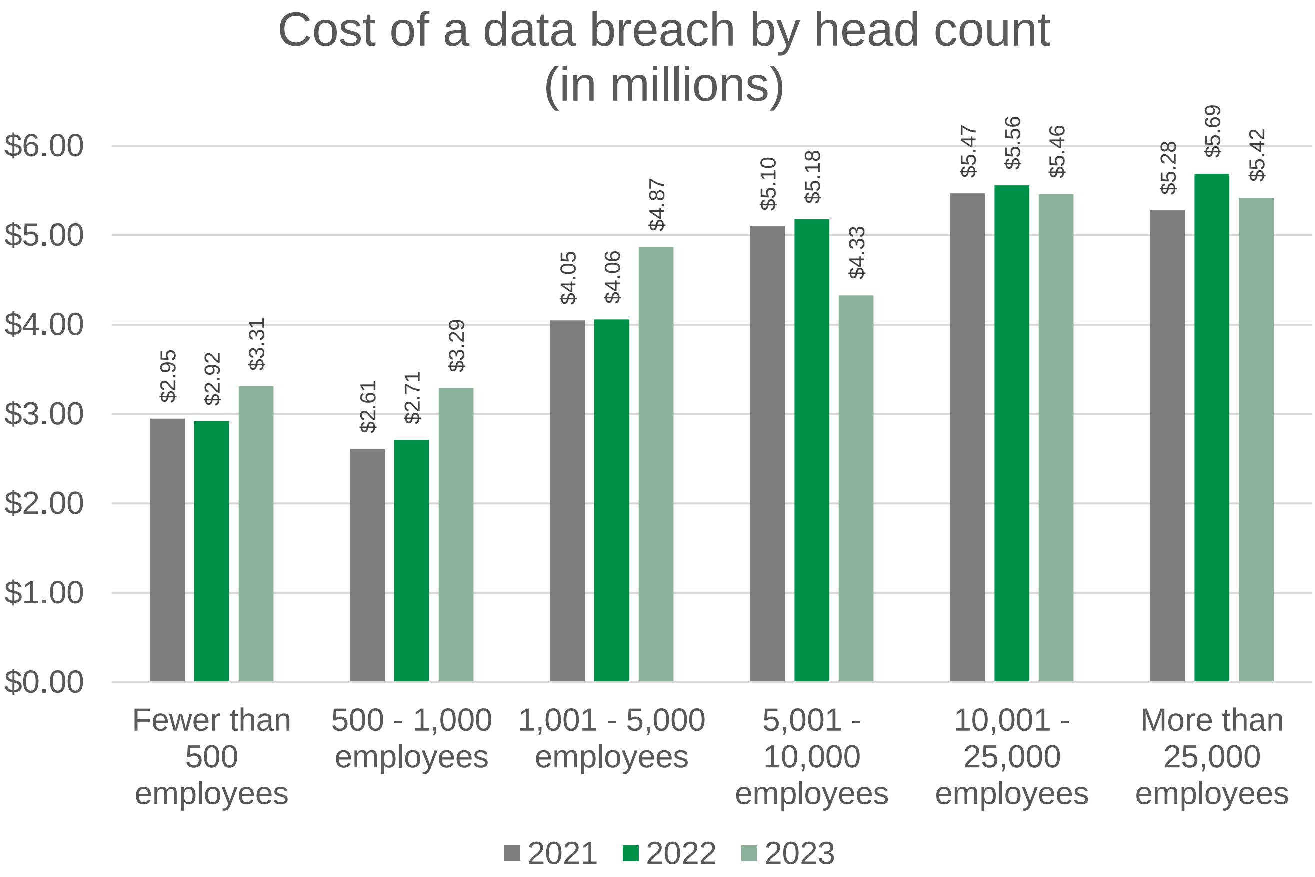
Total Cost of a Breach: $4.45 million

- Up **2.3%** from 2022
- Up **15.3%** from 2020
- Health care data breaches up **53.3%** since 2020
- US average - **$9.48 million**

Source: ibm.com

Size Does Not Matter

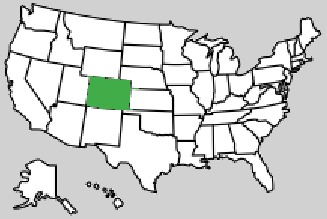
Smaller organizations faced considerably higher data breach costs than last year (13.4%)

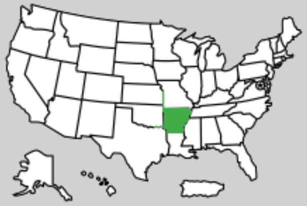


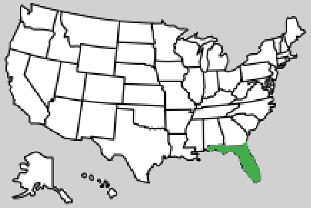
MERS® Municipal Employees' Retirement System

Source: ibm.com

State and Local Government Attacks







Erie, Colorado

- In 2019, the city electronically sent $1 million to a fraudulent account after an impersonator changed the payment preference method for the primary contractor on a local bridge project from check to electronic transfer

Miller County, Arkansas

- Attack in 2022 affected data throughout 55 counties
- No data was extracted, but counties workers were forced to go offline or temporarily close for two weeks until the issue was resolved

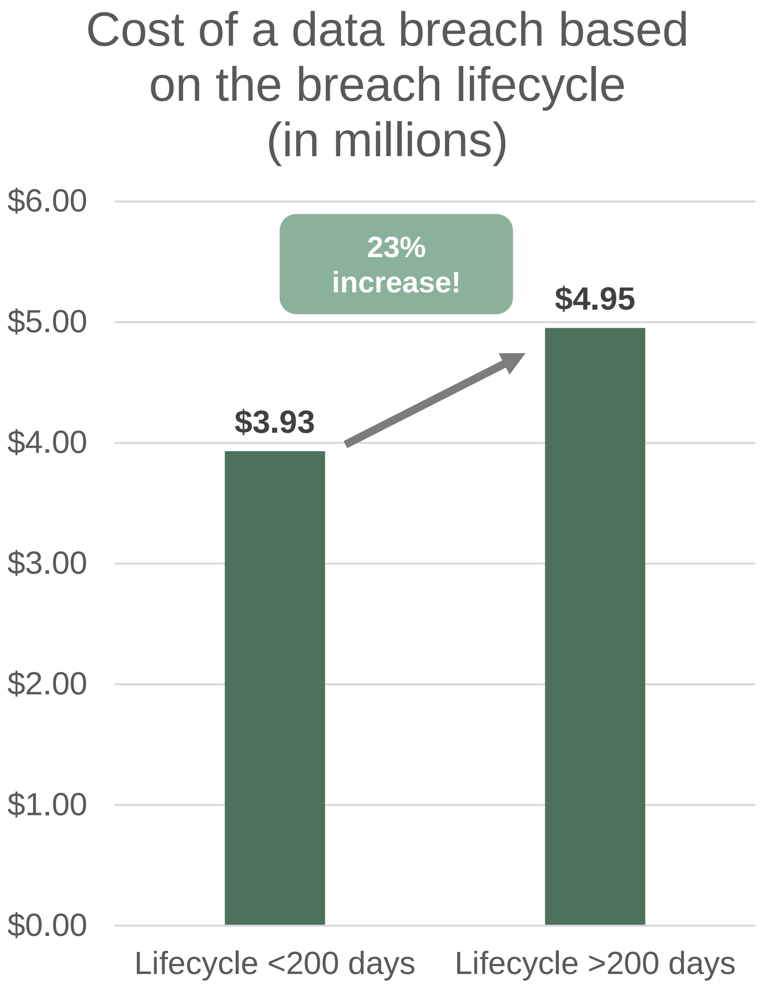
Ocala, Florida

- In 2019, the city fell victim to a spear phishing email that looked like it came from a construction firm working on a new terminal at the city's airport. The city lost more than $740,000

MERS®
Municipal Employees' Retirement System

Source: knowbe4.com

Breach Discovery Timing Matters

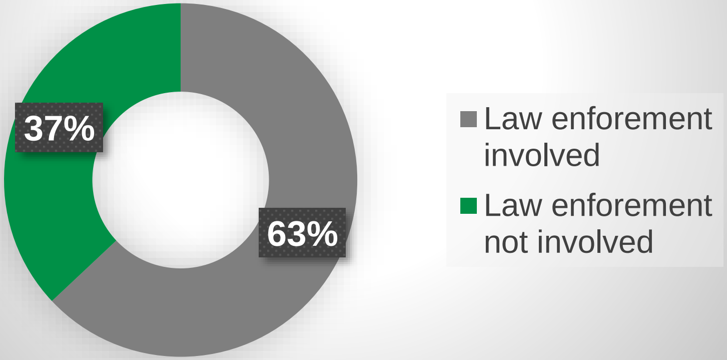


Source: ibm.com

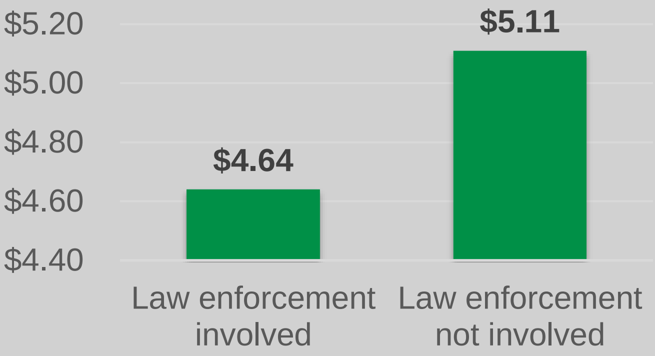
It costs approximately $1.02M less on average if the breach is discovered in less than 200 days

Engaging Law Enforcement

Share of ransomware attacks with law enforcement involved



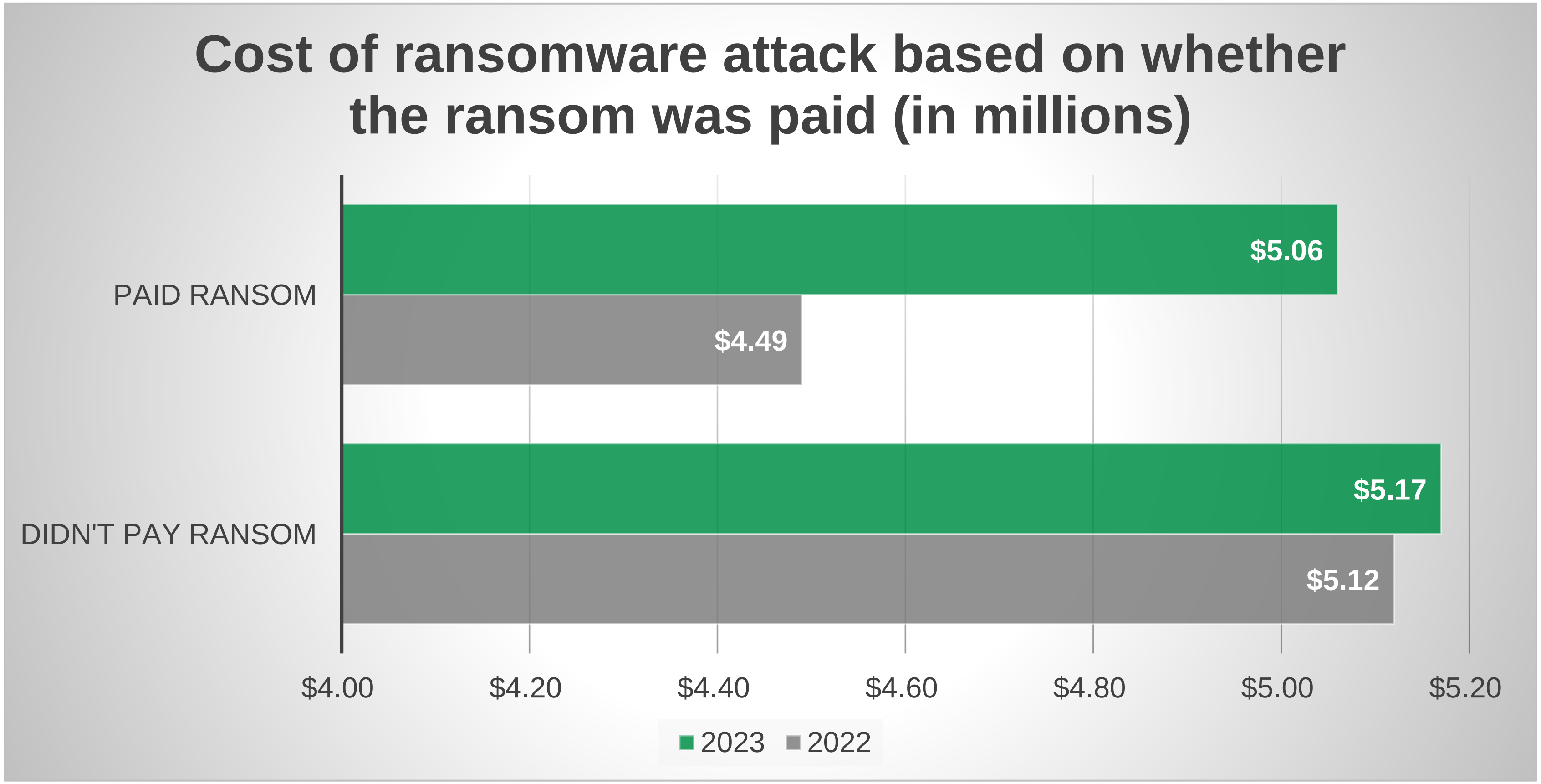
Cost of a ransomware attack by law enforcement involvement (in millions)



Source: ibm.com

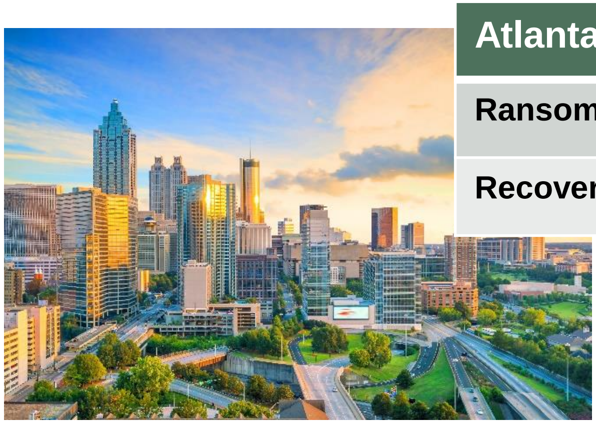
MERS®
Municipal Employees' Retirement System

To Pay, or Not to Pay…



Source: ibm.com

Cities Refusing to Pay Ransom vs. Average Recovery Cost



Atlanta
Ransom Demand: $55,000
Recovery Cost: $17 million

Denver
Ransom Demand: $51,000
Recovery Cost: $1.5 million

Baltimore
Ransom Demand: $76,000
Recovery Cost: $10 - $18 million

New Orleans
Ransom Demand: Unknown
Recovery Cost: $7 - $10 million

Source: KnowB4

Data Recovery and the Propensity to Pay Ransom

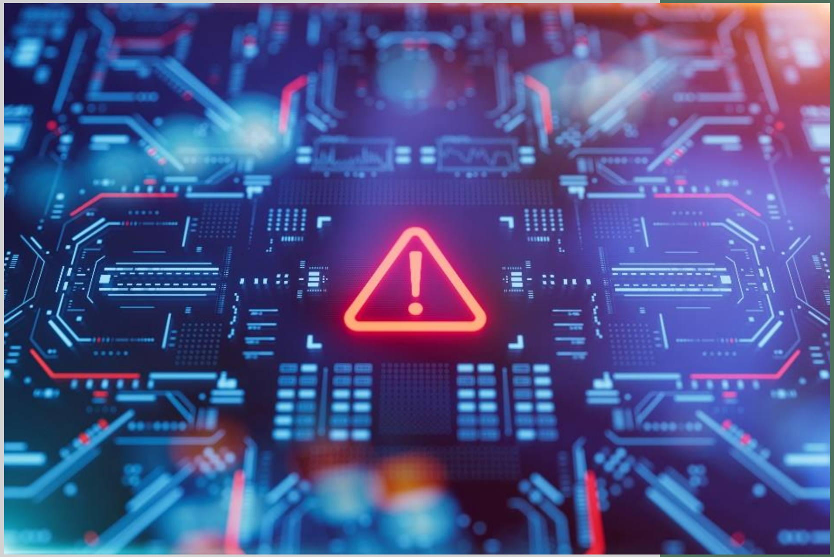
- **99%** of state and local government organizations got their encrypted data back (above the global average of 97%)
- **34%** of organizations reported paying the ransom to recover their encrypted data
- **75%** relied on backups to restore their data. (Up from 63% in 2022 and above the global rate of 70%)
- Ransom demands & payments going up
  - **28%** reported payments of $1 million or more (up from 5%)
  - **60%** paid less than $100,000 (down from 90%)

Source: Sophos

Paying Ransom May Trigger Repeated Attacks

Three additional common reasons for repeated attacks:

1. **Old Vulnerabilities (including backdoors)**
2. **Human error**
3. **Malware**



Source: sophos.com

MERS®
Municipal Employees' Retirement System

Federal Program Provides Aid to Local Communities

- The State and Local Cybersecurity Grant Program (SLCGP) – offered through FEMA - provides about $1B in funding over four years to eligible state, local and territorial (SLT) governments. The purpose is to provide resources that:
  - Manage and reduce systematic cyber risk
  - Improve the security of critical infrastructure
  - Improve the resilience of services provided by SLTs to their communities

Mitigating Your Ransomware Risk

1. **Strengthen defensive shields, including:**

- Security tools that defend against the most common attack vectors
- Adaptive technologies that respond automatically to attacks, disrupting adversaries and buying defenders time to respond
- 24/7 threat detection, investigation and response

2. **Optimize attack preparation**

- Make regular backups
- Practicing recovering data from backups
- Maintain an up-to-date incident response plan

3. **Maintain good security hygiene**

- Timely patching
- Regular review of security tool configurations

MERS®
Municipal Employees' Retirement System

Anti-Ransomware Best Practices

- **Test your disaster recovery process**
- Make sure your backup data is **physically disconnected** from your corporate network
- Make sure you have a **strict vulnerability management process** in place
- Provide your user community with **security awareness training**
- Implement **security controls** on all the systems and devices that may contain company data
- If you must choose between an insurance policy and **increasing your security posture**, do the latter
- **Leverage cyber threat intelligence**

Social Engineering Attack Tactics

Social Engineering

The act of using deception to manipulate individuals into doing something they would not normally do (e.g., divulging confidential or personal information)

- Poison flash drives
- Tailgating
- Phishing

Baiting
Spear phishing
Pretexting
Social engineering
Shoulder surfing
Quid pro quo
Phishing
Tailgating
Dumpster diving
Waling

MERS
Municipal Employees' Retirement System

Phishing

Sending broad emails that look like they are from reputable sources in attempt to get individuals to reveal sensitive personal information.

Common Types:

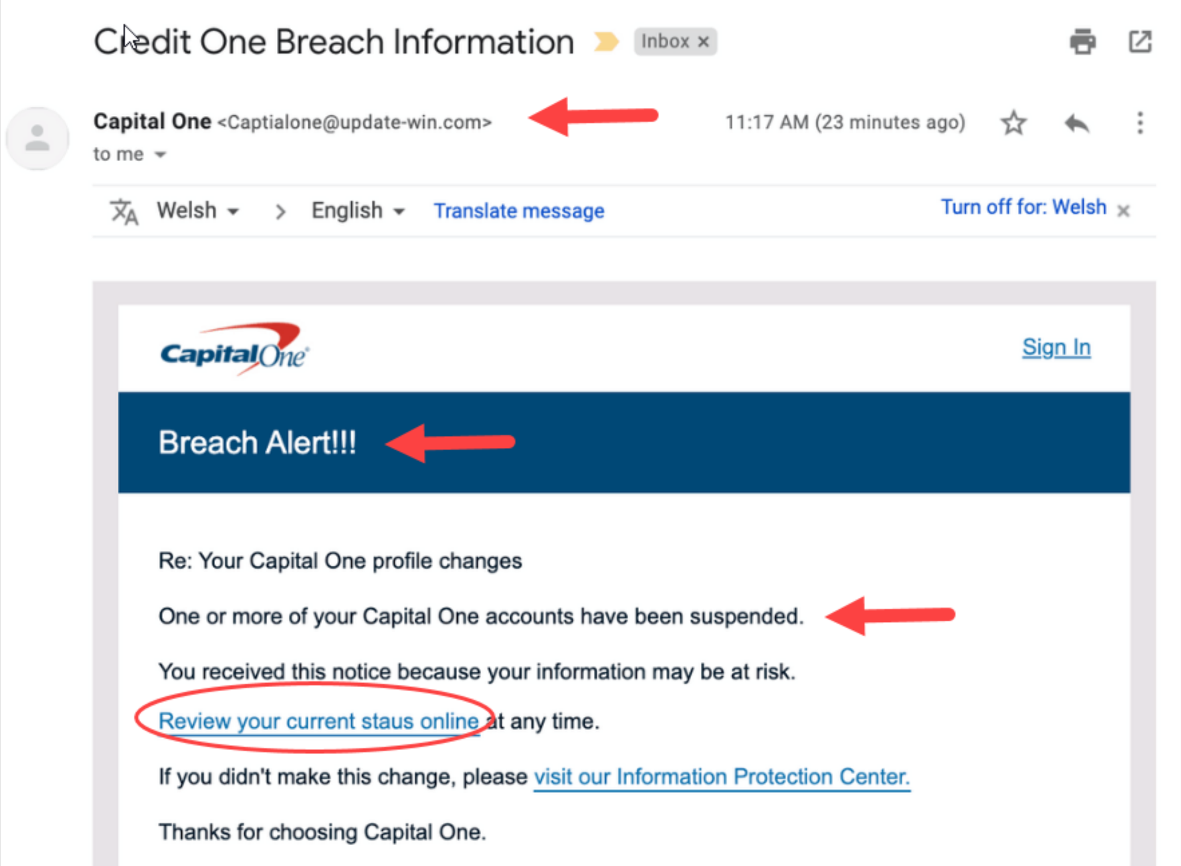
- Spear Phishing – Target a group or individual
- Whaling – Target an executive group or individual
- SMShing – Use text message to manipulate
- Vishing – Use voice to manipulate

Is it a Phishing Email?

Red flags that indicate an email could be “phish bait”:

- **The message is sent from a public email domain**
  - Example: An email from Capital One comes from capitalone@messages.**gmail.com** instead of capitalone@messages.**capitalone.com**
- **The domain name is misspelled**
  - Example: An email from Apple comes from no_reply@email.**appple**.com instead of no_reply@email.**apple**.com
- **The email is poorly written**
  - Misspellings, poor grammar and punctuations mistakes are often signs that an email is phishing.
- **It includes suspicious attachments or links**
- **It includes some sort of scare tactic (You Must Act Now or Something Bad Will Happen!)**

Phishing Email Example



Credit One Breach Information

Capital One <Captialone@update-win.com>

to me

11:17 AM (23 minutes ago)

Breach Alert!!!

Re: Your Capital One profile changes

One or more of your Capital One accounts have been suspended.

You received this notice because your information may be at risk.

Review your current staus online at any time.

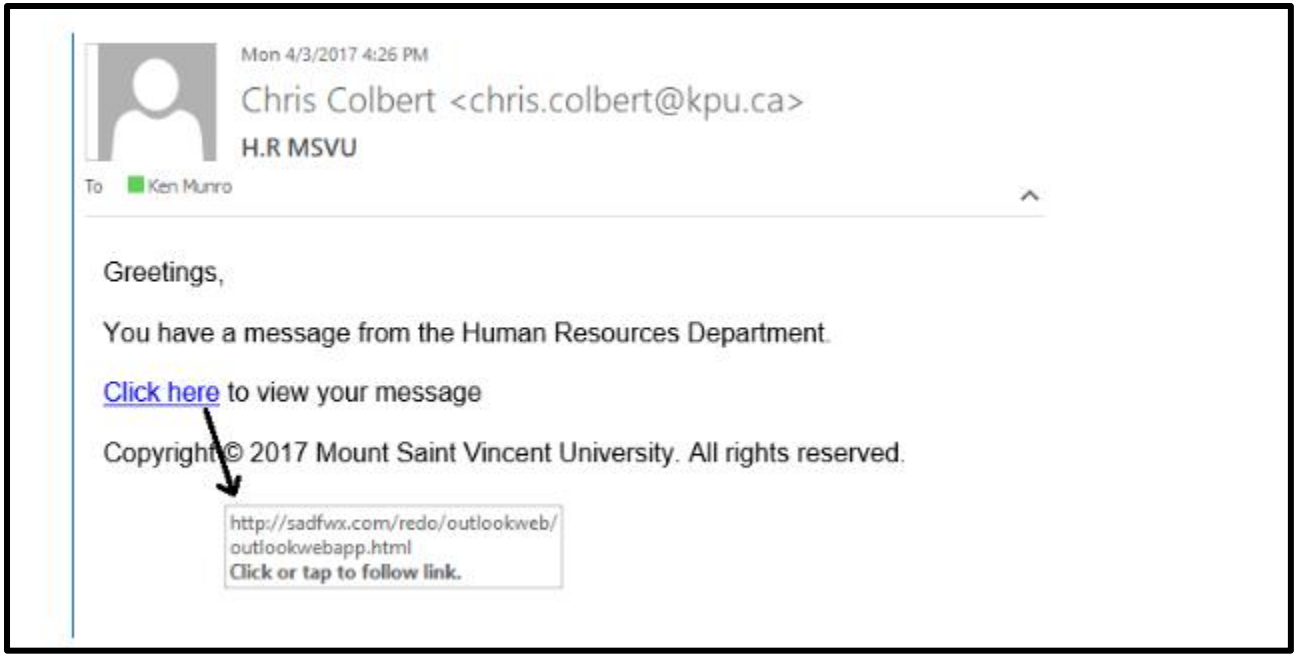
If you didn't make this change, please visit our Information Protection Center.

Thanks for choosing Capital One.

MERS® Municipal Employees' Retirement System

Spear-Phishing Example

FACT:
The most clicked phishing emails by employees are those designed to look like they are coming from their HR department.



Mon 4/3/2017 4:26 PM

Chris Colbert <chris.colbert@kpu.ca>

H.R MSVU

To 🟩 Ken Munro

Greetings,

You have a message from the Human Resources Department.

Click here to view your message

Copyright © 2017 Mount Saint Vincent University. All rights reserved.

http://sadfwx.com/redo/outlookweb/outlookwebapp.html
Click or tap to follow link.

MERS®
Municipal Employees' Retirement System

Source: KnowBe4

Protecting Yourself and Your Family

MERS®
Municipal Employees' Retirement System

How do we fight against an enemy that has:

- More time and resources
- No ethical or moral constraints
- Only need to find one gap in your defenses

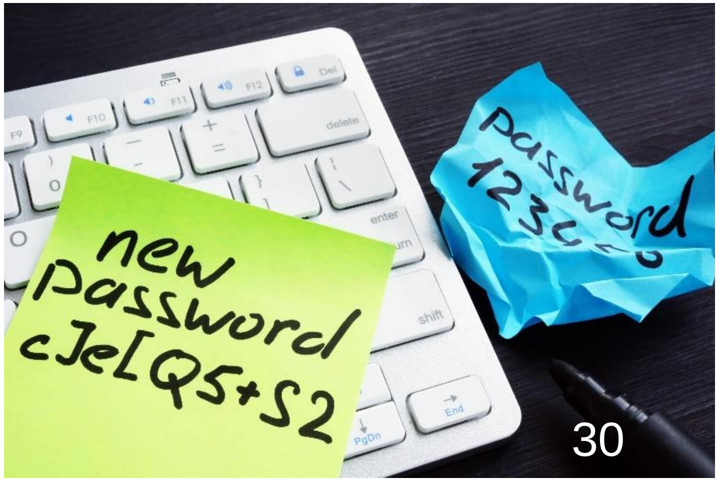
Access Controls and Password Security

- Rather than thinking of your passwords as an annoyance, think of your passwords like your keys, wallet or purse
- Like a wallet or keys, a password is used to prove identity or gain access to a resource and is just as risky to lose

A POOR PASSWORD CAN DIRECTLY IMPACT YOUR WALLET!

“The Trifecta”
Bad Password Mistakes

- **Reuse of passwords**
  - Using the same password for multiple systems
- **Bad password storage and management**
  - Sticky notes, taped under keyboard, an unsecured spreadsheet, not changing passwords within reasonable time frames, etc.
- **Poor password selection**
  - Selecting easily guessed passwords

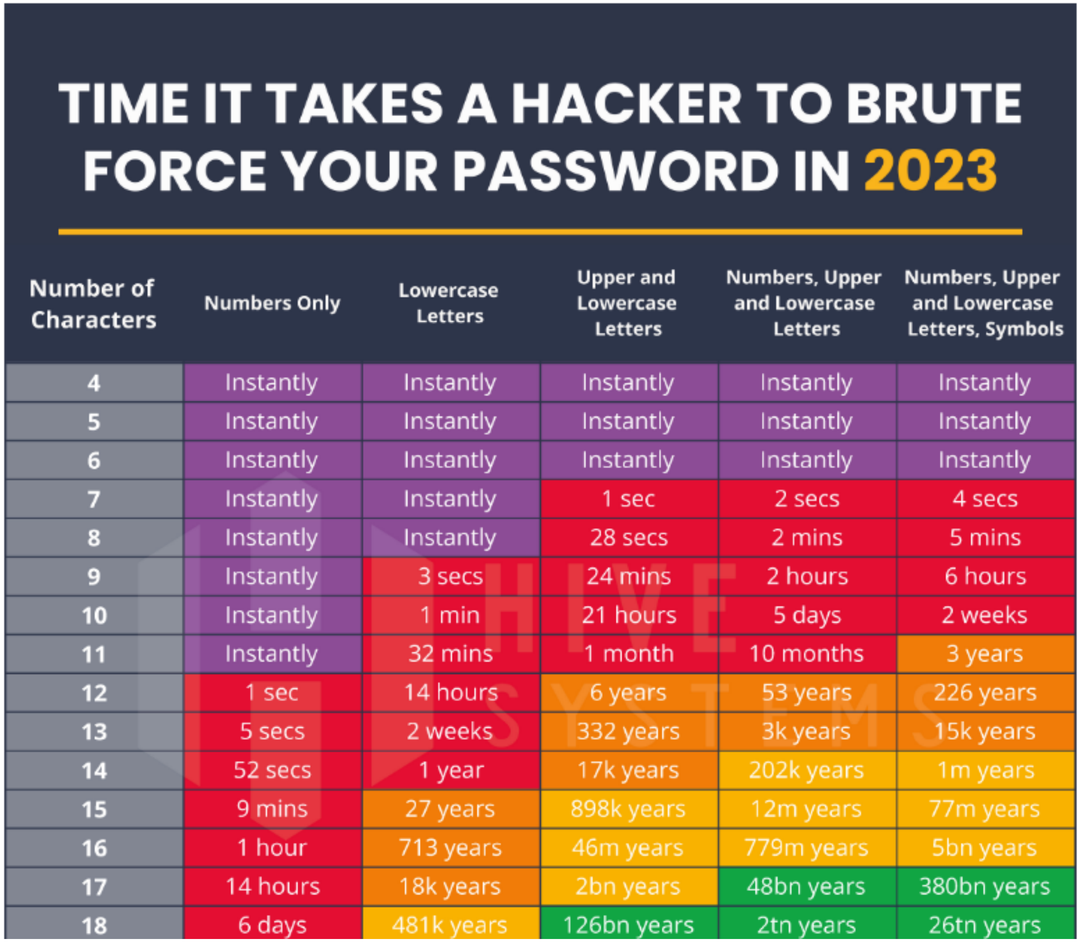


What Makes a Good Password?

- **Examples of good password practices**
  - Use a familiar phrase with phonic/symbol replacements
    IH8P@$$w0rd$
  - The name of the site with phonic/symbol replacements
    MER$0fM1ch
  - Good for managing different passwords for most sites
- **The longer the password, the more secure it is**
  - Using a "passphrase" is the most secure option today
    IH8Entring!0ngP@$$phr@e

Importance of Complex Passwords

How long will it take to hack YOUR password?



TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2023

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	1 sec	2 secs	4 secs
8	Instantly	Instantly	28 secs	2 mins	5 mins
9	Instantly	3 secs	24 mins	2 hours	6 hours
10	Instantly	1 min	21 hours	5 days	2 weeks
11	Instantly	32 mins	1 month	10 months	3 years
12	1 sec	14 hours	6 years	53 years	226 years
13	5 secs	2 weeks	332 years	3k years	15k years
14	52 secs	1 year	17k years	202k years	1m years
15	9 mins	27 years	898k years	12m years	77m years
16	1 hour	713 years	46m years	779m years	5bn years
17	14 hours	18k years	2bn years	48bn years	380bn years
18	6 days	481k years	126bn years	2tn years	26tn years

Source: hivesystems.io

Social Media Dangers

- “TMI” – People are oversharing personal and company information, which can be dangerous

- Targeted “spear phishing” attacks can be built against you, or your family, employees, colleagues or friends based on this type of information

Social Media Do's and Don'ts

DON'T

- Post personally identifiable information (PII), personal health information (PHI), or other sensitive data that can be used for identity theft
- Post information about your organization structure and relationships if not needed
- Post schedule, vacation, or location information unless afterward
- Use the same password for multiple sites

DO

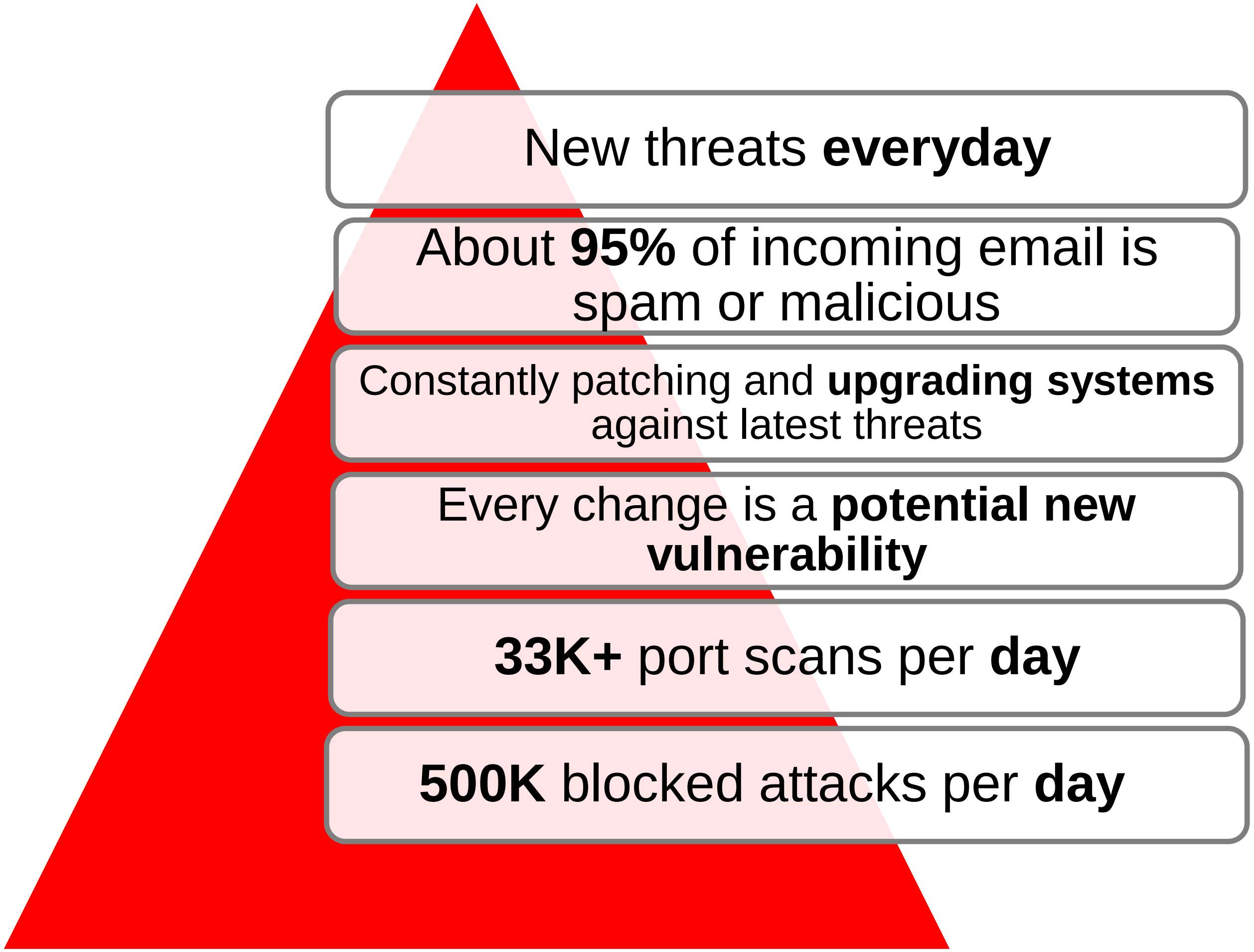
- Use social media sites for intended purpose
- Supply the minimum information necessary to complete your intended purpose
- Understand the personal and professional risks being taken with social media
- Take any cybersecurity training available prior to using social media
- Update privacy settings regularly

MERS®
Municipal Employees' Retirement System

MERS' Cybersecurity Practices

Municipal Employees' Retirement System

“A Day in the Life” of MERS Cybersecurity



New threats **everyday**

About **95%** of incoming email is spam or malicious

Constantly patching and **upgrading systems** against latest threats

Every change is a **potential new vulnerability**

33K+ port scans per **day**

500K blocked attacks per **day**

MERS Cybercrime Defenses

Like most organizations, MERS is in a constant battle to balance **operations** and **security. We use a multi-faceted defense approach to protect data.**

Familiar Defenses

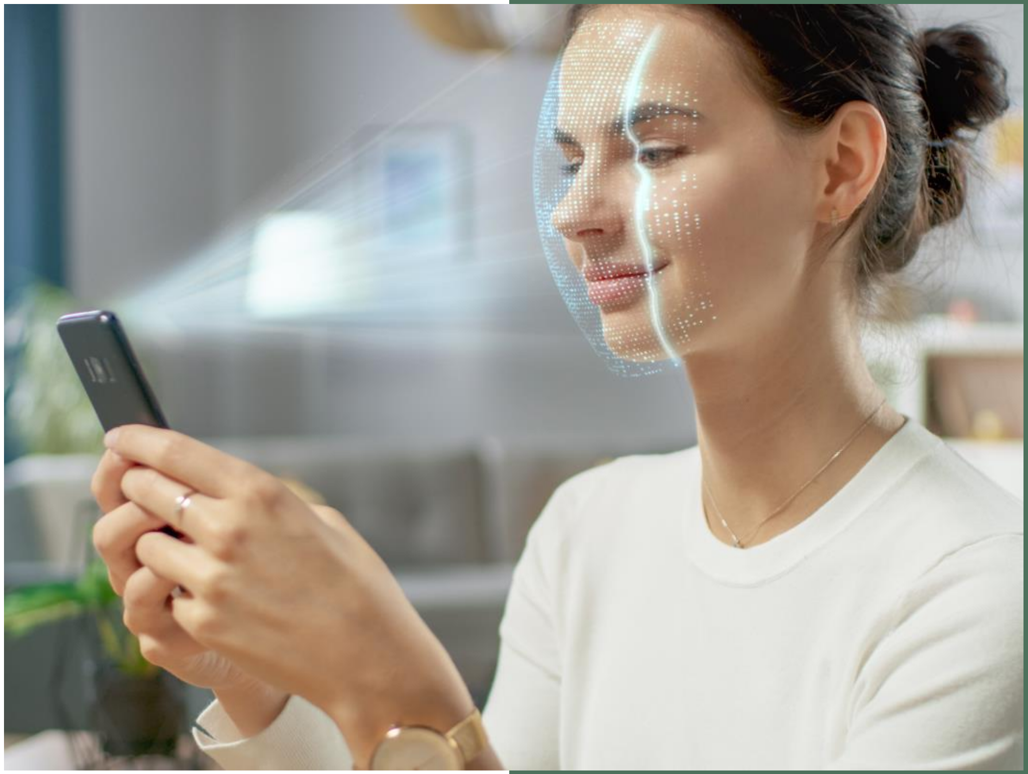
- Anti-virus software (AV)
- Vulnerability scanning software
- Password management software
- Mobile device management software
- Security awareness training
- 2FA access control
- Cyber incident response training

Less Familiar Defenses

- Conditional access controls
- Privileged Access Management
- Network monitoring
- Intrusion Prevention Software (IPS)
- Data Loss Prevention Software (DLP)
- Non-persistent virtual desktops
- Media Access Control (MAC) filtering

MERS®
Municipal Employees' Retirement System

What's Coming: Passwordless Environments



MERS
Municipal Employees' Retirement System

Passwordless Environments

- Instead of using passwords (something the user knows), password less authentication relies on authenticating a user via other means, such as:
  - Something a user has (like a trusted mobile device or a hardware security key)
  - Something they are (for example, scanning their fingerprint, facial recognition, or retina scan)

Passwordless Environments

Companies use passwordless authentication to:

Improve end user experience, as many people forget or reuse unsecured passwords

Reduce security risks to the company stemming from breached passwords

Reduce the cost of maintaining passwords and lifting the burden of password resets on help desk teams

What's Coming: Internet of Things (IoT)

MERS®
Municipal Employees' Retirement System

Understanding IoT

- The Internet of Things (IoT) refers to a network of **physical devices**, **vehicles**, **appliances** and **other physical objects** that are **embedded with sensors, software and network connectivity** that allows them to collect and share data.
- These devices — also known as “smart objects” — can range from simple “smart home” devices like smart thermostats, to wearables like smartwatches and RFID-enabled clothing, to complex industrial machinery and transportation systems.

MERS® Municipal Employees' Retirement System

Source: IBM.com

Future of IoT Cybersecurity

- Enhancing monitoring of devices
- Adding security features
- Following IoT standards

Common IoT Threats

- Inadequate default settings
- Non-existent upgrade paths
- Use of inappropriate technology

What's Coming: Artificial Intelligence (AI)

Understanding AI and ChatGPT

Artificial Intelligence (AI)

- The science of making machines that can think like humans

ChatGPT

- A natural language processing tool driven by AI technology that allows you to have human-like conversations and much more with the chatbot
- Can answer questions and assist you with tasks such as composing emails, essays, and code

Source: zdnet.com

ChatGPT Cybercriminal Adoption

How does ChatGPT factor into cybersecurity?

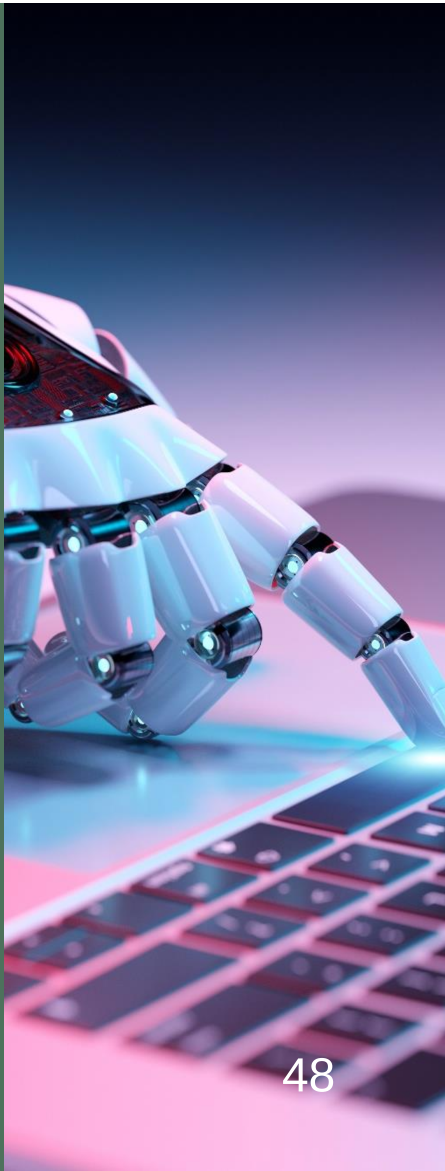
Cybercriminals are using ChatGPT to generate emails with:

- More sophisticated and targeted content
- Improved grammar, spelling, and sentence structure
- Usage of contextually relevant information to increase perception of legitimacy

Protect Yourself from AI-Generated Phishing Emails

- Inspect the sender's email address and domain
- Look for unexpected or unsolicited emails
- Analyze the email's tone, style, and vocabulary
- Examine URLs carefully
- Check for generic greetings or signatures
- Verify email content with the sender
- Use inbound security tools

Source: paubox.com



Next Level Threats

A Style-Based Generator Architecture for Generative Adversarial Networks

Tero Karras, Samuli Laine, Timo Aila

NVIDIA Corporation

https://www.youtube.com/watch?v=StoMntXhy7s

MERS of Michigan

1134 Municipal Way
Lansing, MI 48917

800.767.6377

www.mersofmich.com

This presentation contains a summary description of MERS benefits, policies or procedures. MERS has made every effort to ensure that the information provided is accurate and up to date. Where the publication conflicts with the relevant Plan Document, the Plan Document controls.