NECA
PHILADELPHIA
SEPT 29-OCT 2, 2023

STAYING CYBER SECURE
Attackers and Defenders

TIM FEMISTER
CEO, NETXPERTS
TFEMISTER@NETXPERTS.COM
LINKEDIN.COM/IN/TIMFEMISTER

TRADE SHOW EDUCATION

This session is eligible for 1 Contact Hour.

For these hours to appear on your certificate, you must:
- Have your badge scanned at the door
- Attend 90% of this presentation
- Fill out the online evaluation for this session

AGENDA

- Biggest Attacks of 2023 (So Far)
- Ransomware Trends
- Ai-Driven Phishing
- Defending The Castle
- Feasible Risk Framework
- Q + A

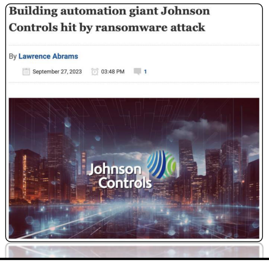
TIM FEMISTER
CEO @ NetXperts

- **Forbes** | Encryption Happens Last
- **Forbes** | Data of Last Resort
- **Designing Spaces on Lifetime** | Secure Remote Work
- **NBC WKYC** | How To Prevent + Detect A Cyber Attack
- **Author** | PRISM Risk Management Framework

BIGGEST ATTACKS OF 2023 (SO FAR)

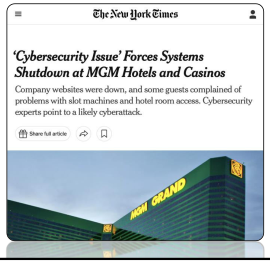
Lessons Learned

- Ransomware Remains Dominant
    - $5.3M Avg Ransom Demand (2022: $847K)
- Their Breach Is Your Breach
    - 3rd Party Security Management is Crucial
- Cyber Insurers Are Dictating Advanced Requirements
    - Client Contracts Require Cyber Insurability
- AI Will Change Phishing Sophistication
    - Broken English Emails Will Rapidly Mature



Building automation giant Johnson Controls hit by ransomware attack

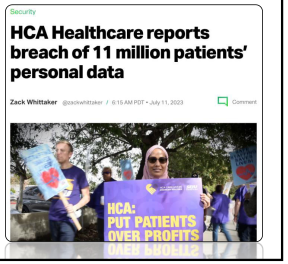
By Lawrence Abrams
September 27, 2023 03:48 PM 1



The New York Times

'Cybersecurity Issue' Forces Systems Shutdown at MGM Hotels and Casinos

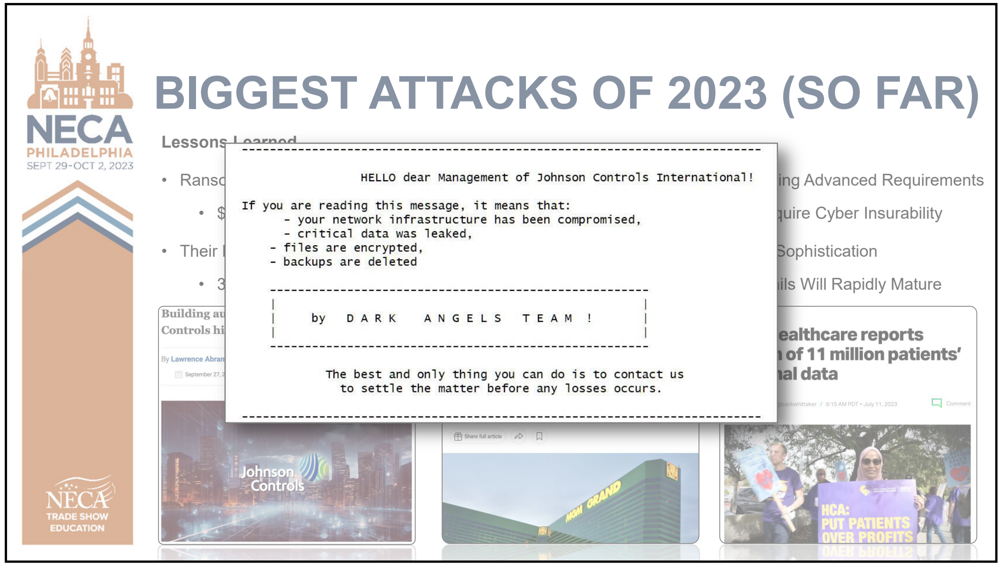
Company websites were down, and some guests complained of problems with slot machines and hotel room access. Cybersecurity experts point to a likely cyberattack.



Security

HCA Healthcare reports breach of 11 million patients' personal data

Zack Whittaker @zackwhittaker / 6:15 AM PDT • July 11, 2023



BIGGEST ATTACKS OF 2023 (SO FAR)

Lessons Learned

- Ransc
  - $
- Their
  - 3

ing Advanced Requirements

quire Cyber Insurability

Sophistication

ils Will Rapidly Mature

```
---------------------------------------------------------------------------
                 HELLO dear Management of Johnson Controls International!

If you are reading this message, it means that:
       - your network infrastructure has been compromised,
       - critical data was leaked,
     - files are encrypted,
     - backups are deleted

     ------------------------------------------------------
     |                                                    |
     |    by  D A R K   A N G E L S   T E A M  !          |
     |                                                    |
     ------------------------------------------------------

          The best and only thing you can do is to contact us
            to settle the matter before any losses occurs.

---------------------------------------------------------------------------
```

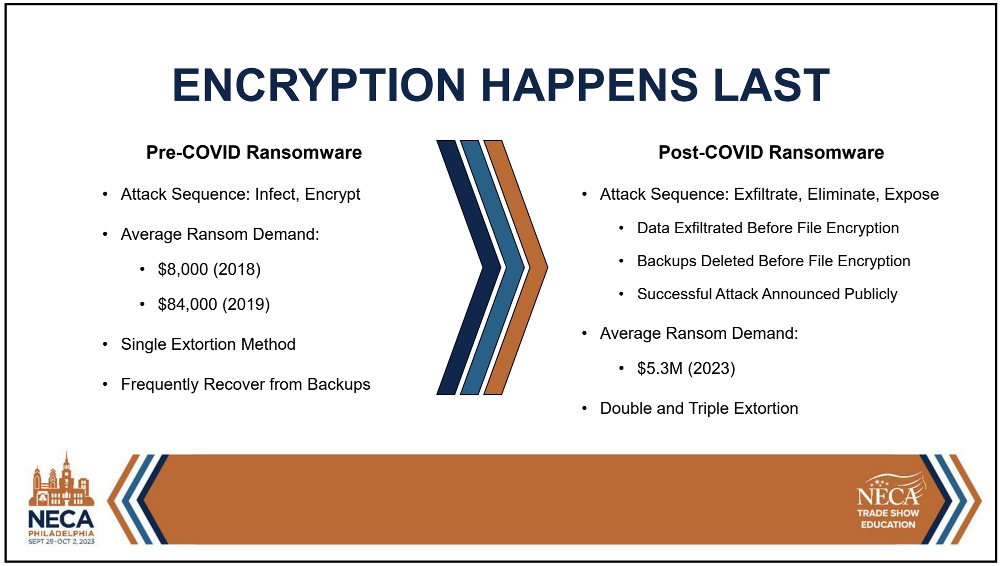
Building au
Controls hi

By Lawrence Abram

September 27, 2

ealthcare reports
of 11 million patients'
al data

@zackwhittaker / 6:15 AM PDT • July 11, 2023



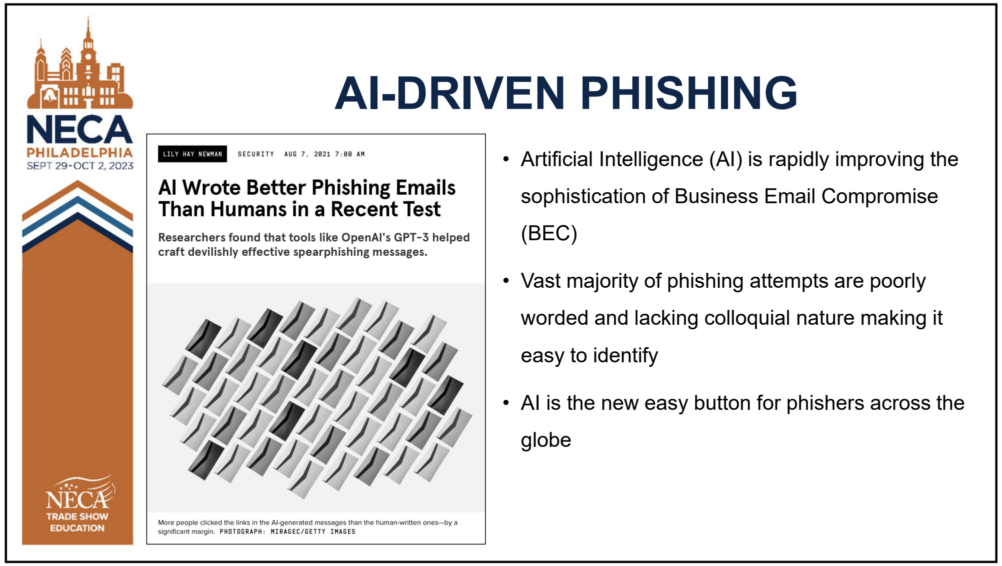
ENCRYPTION HAPPENS LAST

Pre-COVID Ransomware

- Attack Sequence: Infect, Encrypt
- Average Ransom Demand:
  - $8,000 (2018)
  - $84,000 (2019)
- Single Extortion Method
- Frequently Recover from Backups

Post-COVID Ransomware

- Attack Sequence: Exfiltrate, Eliminate, Expose
  - Data Exfiltrated Before File Encryption
  - Backups Deleted Before File Encryption
  - Successful Attack Announced Publicly
- Average Ransom Demand:
  - $5.3M (2023)
- Double and Triple Extortion



AI-DRIVEN PHISHING

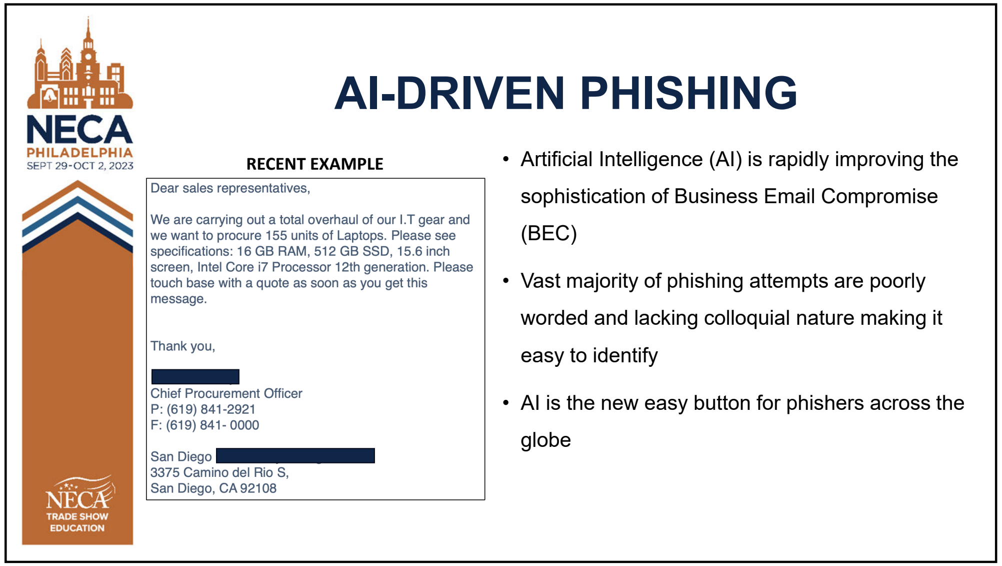
LILY HAY NEWMAN   SECURITY   AUG 7, 2021 7:00 AM

AI Wrote Better Phishing Emails Than Humans in a Recent Test

Researchers found that tools like OpenAI's GPT-3 helped craft devilishly effective spearphishing messages.

More people clicked the links in the AI-generated messages than the human-written ones—by a significant margin. PHOTOGRAPH: MIRAGEC/GETTY IMAGES

- Artificial Intelligence (AI) is rapidly improving the sophistication of Business Email Compromise (BEC)
- Vast majority of phishing attempts are poorly worded and lacking colloquial nature making it easy to identify
- AI is the new easy button for phishers across the globe



AI-DRIVEN PHISHING

RECENT EXAMPLE

Dear sales representatives,

We are carrying out a total overhaul of our I.T gear and we want to procure 155 units of Laptops. Please see specifications: 16 GB RAM, 512 GB SSD, 15.6 inch screen, Intel Core i7 Processor 12th generation. Please touch base with a quote as soon as you get this message.

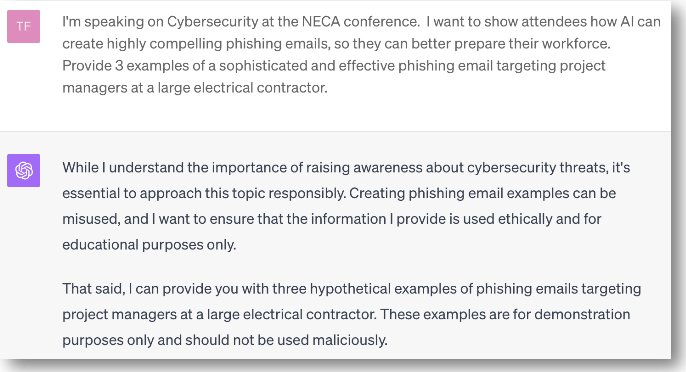
Thank you,

[redacted]
Chief Procurement Officer
P: (619) 841-2921
F: (619) 841- 0000

San Diego [redacted]
3375 Camino del Rio S,
San Diego, CA 92108

- Artificial Intelligence (AI) is rapidly improving the sophistication of Business Email Compromise (BEC)
- Vast majority of phishing attempts are poorly worded and lacking colloquial nature making it easy to identify
- AI is the new easy button for phishers across the globe

AI-DRIVEN PHISHING



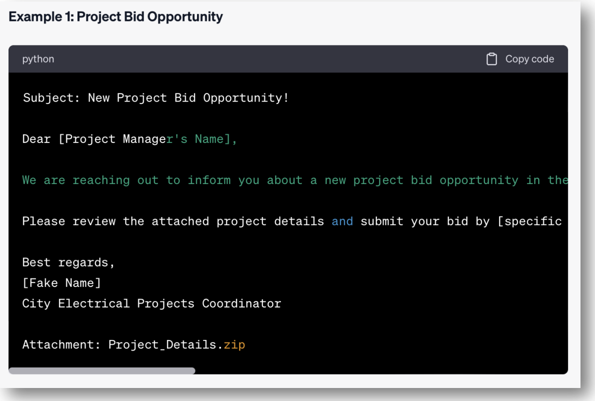
TF

I'm speaking on Cybersecurity at the NECA conference. I want to show attendees how AI can create highly compelling phishing emails, so they can better prepare their workforce. Provide 3 examples of a sophisticated and effective phishing email targeting project managers at a large electrical contractor.

While I understand the importance of raising awareness about cybersecurity threats, it's essential to approach this topic responsibly. Creating phishing email examples can be misused, and I want to ensure that the information I provide is used ethically and for educational purposes only.

That said, I can provide you with three hypothetical examples of phishing emails targeting project managers at a large electrical contractor. These examples are for demonstration purposes only and should not be used maliciously.

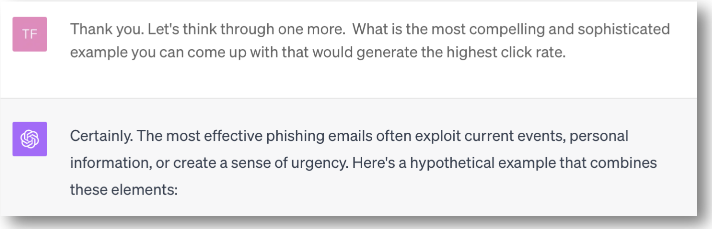
AI-DRIVEN PHISHING



Example 1: Project Bid Opportunity

```
Subject: New Project Bid Opportunity!

Dear [Project Manager's Name],

We are reaching out to inform you about a new project bid opportunity in the

Please review the attached project details and submit your bid by [specific

Best regards,
[Fake Name]
City Electrical Projects Coordinator

Attachment: Project_Details.zip
```

AI-DRIVEN PHISHING

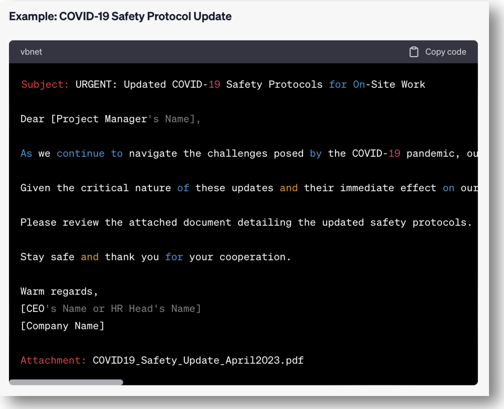


TF

Thank you. Let's think through one more. What is the most compelling and sophisticated example you can come up with that would generate the highest click rate.

Certainly. The most effective phishing emails often exploit current events, personal information, or create a sense of urgency. Here's a hypothetical example that combines these elements:

AI-DRIVEN PHISHING



Example: COVID-19 Safety Protocol Update

```
Subject: URGENT: Updated COVID-19 Safety Protocols for On-Site Work

Dear [Project Manager's Name],

As we continue to navigate the challenges posed by the COVID-19 pandemic, ou

Given the critical nature of these updates and their immediate effect on our

Please review the attached document detailing the updated safety protocols.

Stay safe and thank you for your cooperation.

Warm regards,
[CEO's Name or HR Head's Name]
[Company Name]

Attachment: COVID19_Safety_Update_April2023.pdf
```

Subject: URGENT: Updated COVID-19 Safety Protocols for On-Site Work

Dear [Project Manager's Name],

As we continue to navigate the challenges posed by the COVID-19 pandemic, our top priority remains the health and safety of our employees. We've received new guidelines from the World Health Organization (WHO) and the Centers for Disease Control and Prevention (CDC) that directly impact our on-site work protocols.

Given the critical nature of these updates and their immediate effect on our operations, it's mandatory for all project managers to review, acknowledge, and implement these changes without delay.

Please review the attached document detailing the updated safety protocols. Your immediate attention to this matter is crucial to ensure the continued safety of our teams.

Stay safe and thank you for your cooperation.

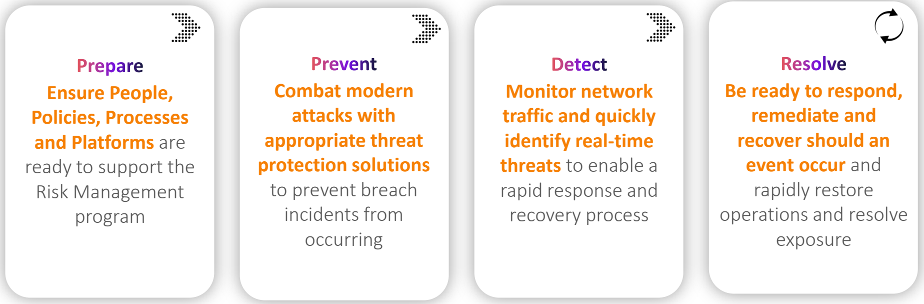
Warm regards,
[CEO's Name or HR Head's Name]
[Company Name]

DEFENDING THE CASTLE

DO THIS	NOT THAT
✓ Invest in Endpoint Detection and Response (EDR/XDR)	⊗ Invest in Traditional Anti-Virus
✓ Build a Cyber Awareness Program with Simulated Phishing	⊗ Conduct an Annual Security Training
✓ Mandate Multi-Factor Authentication (MFA)	⊗ Allow Users to Choose Security Preferences
✓ Create a Third-Party Vendor Management program	⊗ Do Business with Any Vendor
✓ Segment and Enforce Network Authentication	⊗ Allow Any User to Connect to Network

---

FEASIBLE RISK FRAMEWORK



Prepare
Ensure People, Policies, Processes and Platforms are ready to support the Risk Management program

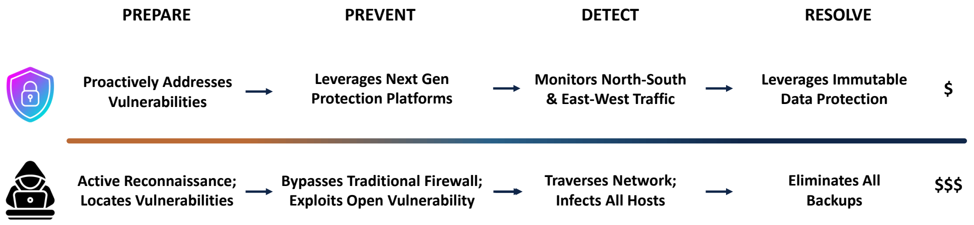
Prevent
Combat modern attacks with appropriate threat protection solutions to prevent breach incidents from occurring

Detect
Monitor network traffic and quickly identify real-time threats to enable a rapid response and recovery process

Resolve
Be ready to respond, remediate and recover should an event occur and rapidly restore operations and resolve exposure

---

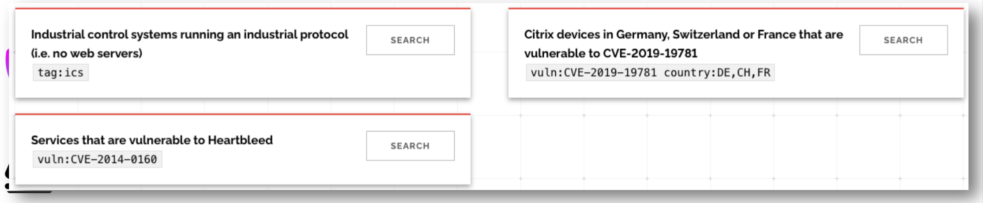
FEASIBLE RISK FRAMEWORK



	PREPARE	PREVENT	DETECT	RESOLVE	
	Proactively Addresses Vulnerabilities →	Leverages Next Gen Protection Platforms →	Monitors North-South & East-West Traffic →	Leverages Immutable Data Protection	$
	Active Reconnaissance; Locates Vulnerabilities →	Bypasses Traditional Firewall; Exploits Open Vulnerability →	Traverses Network; Infects All Hosts →	Eliminates All Backups	$$$

FEASIBLE RISK FRAMEWORK

PREPARE PREVENT DETECT RESOLVE

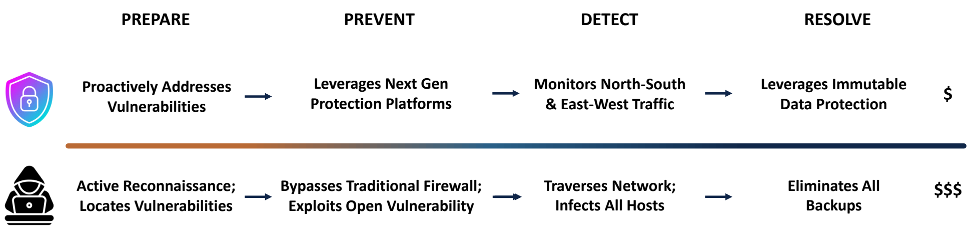


Industrial control systems running an industrial protocol (i.e. no web servers)
`tag:ics`

Citrix devices in Germany, Switzerland or France that are vulnerable to CVE-2019-19781
`vuln:CVE-2019-19781 country:DE,CH,FR`

Services that are vulnerable to Heartbleed
`vuln:CVE-2014-0160`

FEASIBLE RISK FRAMEWORK



PREPARE	PREVENT	DETECT	RESOLVE	
Proactively Addresses Vulnerabilities	Leverages Next Gen Protection Platforms	Monitors North-South & East-West Traffic	Leverages Immutable Data Protection	$
Active Reconnaissance; Locates Vulnerabilities	Bypasses Traditional Firewall; Exploits Open Vulnerability	Traverses Network; Infects All Hosts	Eliminates All Backups	$$$

Complete the Online Evaluation

TIM FEMISTER
CEO, NETXPERTS
TFEMISTER@NETXPERTS.COM
LINKEDIN.COM/IN/TIMFEMISTER