

THE BUSINESS OF CYBERCRIME

58th Annual County Finance School

May 1-3, 2024

Turning Stone Resort, Verona, NY



Sponsored by:

NYS Association of Counties

Office of the State Comptroller

NYS Treasurers and Finance Officers Association

WITH YOU TODAY FROM NYSTEC



 **Joel Djanie**

(917) 946-4890 - Mobile

jdjanie@nystec.com



 **Jeannine Jacobs**

(518) 588-4343

jjacobs@nystec.com



 **Slawomir Marcinkowski**

(315) 243-0428 - Mobile

smarcinkowski@nystec.com



 **Jeffrey Wilson**

(518) 210-8539 - Cell

jwilson@nystec.com



 **Rob Zeglen**

(518) 368-4277

rzeglen@nystec.com

NYS TECHNOLOGY ENTERPRISE CORPORATION



Who We Are



Incorporated in 1996 as
Systems Engineering and
Technical Assistance
(SETA) advisor



Private nonprofit
information technology
consulting company



Help make a positive impact
in New York State
communities



NYSTEC



What We Do



BUSINESS ANALYSIS

Identify and clearly state the need for change in how your organization works and how to make that change happen.



DATA STRATEGY & ANALYSIS

Use, share, and store data securely to help you meet your business objectives.



INFORMATION EXCHANGE

Share and access information securely between systems and organizations.



INNOVATION & ENTREPRENEURSHIP

Think and act in dynamic ways to take your business to the next level.



ORGANIZATIONAL CHANGE MANAGEMENT

Develop tailored solutions to help your stakeholders understand and adopt organizational change.



PROGRAM & PROJECT MANAGEMENT

Provide certified program and project managers to oversee your complex endeavors and help orchestrate your initiative's moving parts.



QUALITY CONTROL & ASSURANCE

Improve the effectiveness of your risk management, control, and governance processes.



SECURITY & PRIVACY

Keep your information assets safe, secure, and compliant with federal, state, and organizational regulations.



STRATEGIC PLANNING

Define strategy or direction and determine how to achieve strategic goals.



TECHNICAL ARCHITECTURE & COMMUNICATIONS SYSTEMS

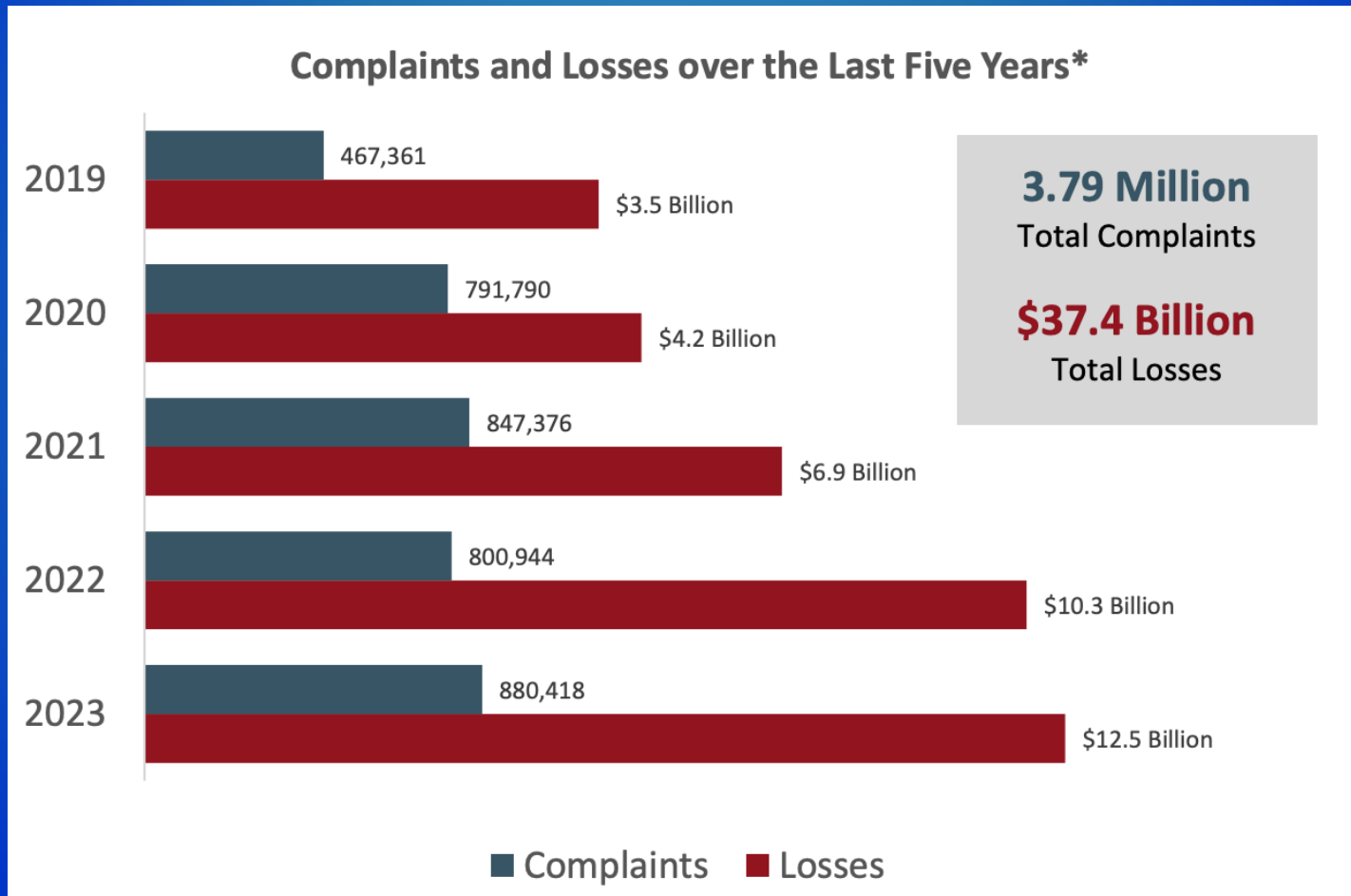
Establish and enhance your networks, systems, and communications or your preferred technologies and platforms.



TECHNOLOGY ACQUISITIONS

Guide you through the entire acquisition process for new technologies or replacement systems.

CYBERSECURITY AND FINANCE



The Business of Cybercrime

Is your Organization in Jeopardy?

*TODAY'S JEOPARDY! GAME IS NOT AUTHORIZED BY JEOPARDY!
PRODUCTIONS, SONY PICTURES OR MERV GRIFFIN*

Start

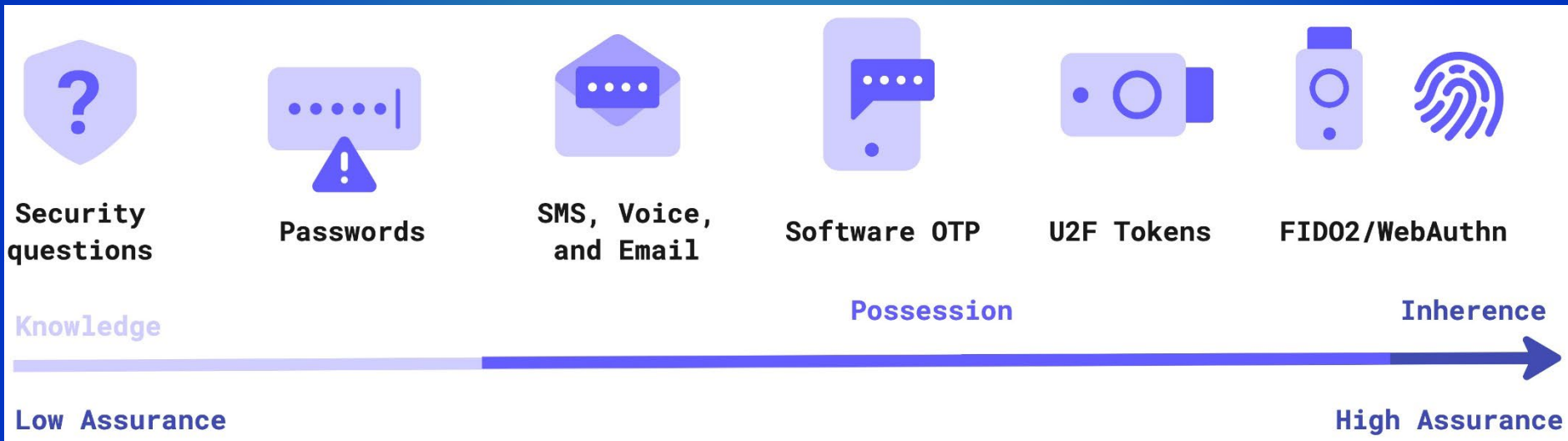
CYBER HYGIENE BEST PRACTICES	CYBER CRIME 101	CYBER INSURANCE	GONE PHISHING	MANDATORY AI CATEGORY
<u>\$200</u>	<u>\$200</u>	<u>\$200</u>	<u>\$200</u>	<u>\$200</u>
<u>\$400</u>	<u>\$400</u>	<u>\$400</u>	<u>\$400</u>	<u>\$400</u>
<u>\$600</u>	<u>\$600</u>	<u>\$600</u>	<u>\$600</u>	<u>\$600</u>
<u>\$800</u>	<u>\$800</u>	<u>\$800</u>	<u>\$800</u>	<u>\$800</u>

SOMETHING YOU KNOW
SOMETHING YOU HAVE
SOMETHING YOU ARE

Answer



WHAT IS MULTIFACTOR AUTHENTICATION?



<https://www.nist.gov/itl/smallbusinesscyber/guidance-topic/multi-factor-authentication>



THIS IS A QUALITATIVE OR
QUANTITATIVE ESTIMATE OF
POTENTIAL IMPACT FROM A
THREAT OR HAZARD RELATED
TO A RECOGNIZED
VULNERABILITY.

Answer

WHAT IS A RISK ASSESSMENT?



**SOMETHING EVERY
ORGANIZATION MUST HAVE IN
PLACE TO PROPERLY RESPOND
TO A CYBER INCIDENT.**

Answer

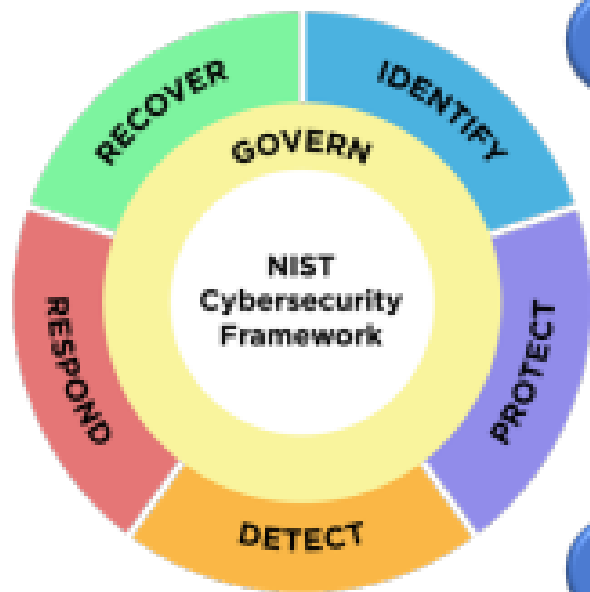
WHAT IS AN INCIDENT RESPONSE PLAN?



**THIS NIST INFORMATION
SECURITY POLICY FRAMEWORK
HELPS PRIVATE SECTOR
ORGANIZATIONS IMPROVE
THEIR ABILITY TO PREVENT,
DETECT, AND RESPOND TO
CYBER ATTACKS.**

Answer

WHAT IS THE NIST CYBERSECURITY FRAMEWORK (CSF)?



- 1 Scope the Organizational Profile
- 2 Gather needed information
- 3 Create the Organizational Profile
- 4 Analyze gaps and create an action plan
- 5 Implement action plan and update Profile

Repeat...

<https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf>



THESE ATTACKS ON FINANCIAL INSTITUTIONS INCREASED FROM 55% IN 2022 TO 64% IN 2023, AND ONLY 1 OUT OF 10 WERE STOPPED BEFORE DATA WAS RENDERED UNAVAILABLE.

Answer

WHAT IS RANSOMWARE?



- <https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view>



**IN THIS CYBERCRIME BUSINESS
MODEL ONE CRIMINAL GANG
SELLS CODE OR MALWARE TO
OTHER HACKERS, WHO THEN
USE IT TO CARRY OUT
CYBERATTACKS.**

Answer

**WHAT IS RANSOMWARE AS A
SERVICE (RAAS)?**



PEDDLERS



PEDDLERS



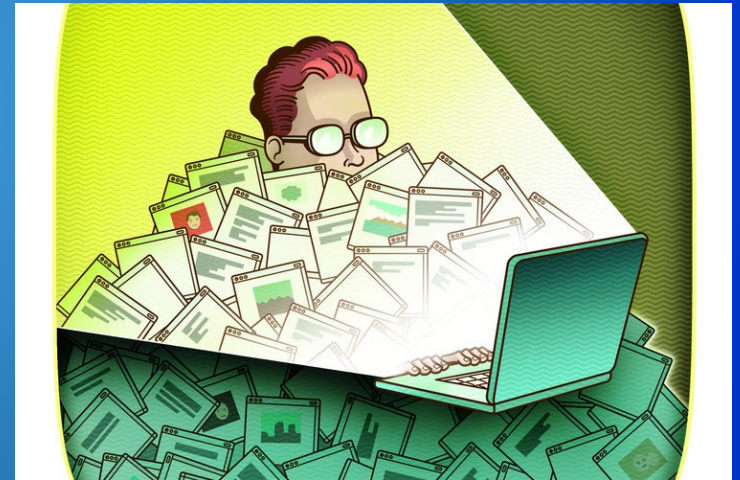
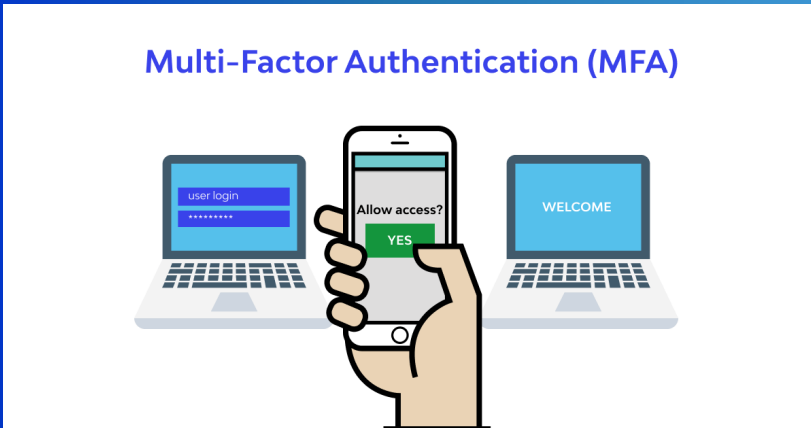
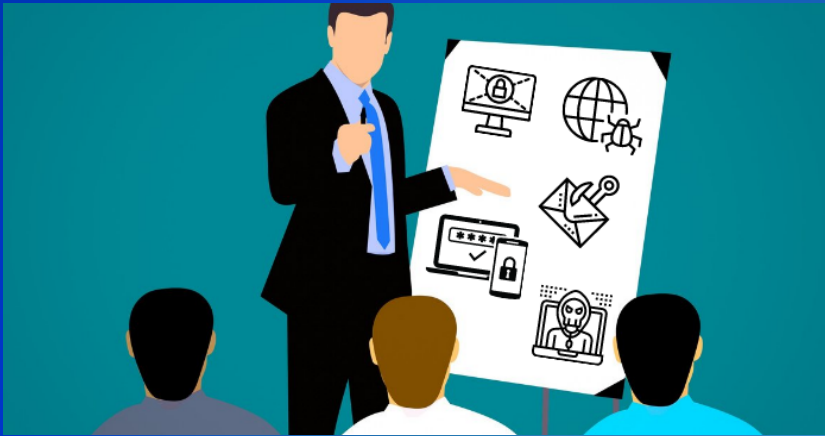
©2021 TREND MICRO



**THIS TYPE OF EMAIL ATTACK,
TARGETING BOTH BUSINESSES
AND INDIVIDUALS, RESULTED IN
ADJUSTED LOSSES OF OVER \$2.9B
IN 2023.**

Answer

WHAT IS BUSINESS EMAIL COMPROMISE (BEC)?



**LOSSES RELATED TO THIS
FINANCIAL SCAM WERE THE
HIGHEST OF ANY CRIME TYPE IN
2023, SEEING A 38% INCREASE IN
JUST ONE YEAR.**

Answer

WHAT ARE INVESTMENT SCAMS?



**AN ORGANIZATION MAY
CHOOSE TO OFFSET COSTS
ASSOCIATED WITH CYBER-
RELATED INCIDENTS BY
TRANSFERRING RISK THROUGH
THIS METHOD.**

Answer

WHAT IS CYBER INSURANCE?



**CYBER INSURANCE GENERALLY
CONSISTS OF THESE TWO TYPES
OF POLICIES.**

Answer

WHAT ARE FIRST- AND THIRD- PARTY COVERAGE?

CYBER LIABILITY INSURANCE COVERAGES

FIRST PARTY COVERAGE

Direct Loss incurred by your business because of "injury" to electronic data or systems resulting from acts of others

- Recovery of compromised data
- Theft of data and intangible property
- Business Interruption
- Extortion

THIRD PARTY COVERAGE

Liability for financial losses or costs sustained by third parties who have been impacted by data breach

- Legal fees incurred to protect the business against claims from customers for personal/content injury, intellectual property claims, professional services, from a security or privacy breach
- Regulatory fines/penalties



TO QUALIFY FOR CYBER
INSURANCE, ORGANIZATIONS
MUST DEMONSTRATE THAT
THEY HAVE THIS.

Answer

WHAT IS A STRONG CYBER SECURITY PROGRAM?



**CYBER INSURANCE AND CYBER
SECURITY PROGRAMS ARE TWO
COMPONENTS OF THIS
ESSENTIAL PART OF
ORGANIZATIONAL PLANNING.**

Answer

WHAT IS A RISK MANAGEMENT STRATEGY?



**THIS TYPE OF PHISHING ATTACK
IS DIRECTED AT SPECIFIC
INDIVIDUALS USING PERSONAL
AND COMPANY INFORMATION
GATHERED FROM SOCIAL MEDIA**

Answer

WHAT IS SPEAR FISHING?

Did you know that 91% of successful data breaches started with a spear phishing attack?

Spear Phishing Psychological Triggers

- Authority
- Urgency
- Curiosity
- Familiarity
- Fear

[The Top 5 Spear Phishing Examples and Their Psychological Triggers - Hornetsecurity – Cloud Security Services for Businesses](#)



PHISHING VS SPEAR PHISHING

Approach	Spray and pray	Targeted attack
Targeting	Broad and automated	Specific employee and/or company
Hacking Level	Not very sophisticated	Requires advanced techniques
The Attack	Usually obvious	Harder to detect
What They Are After	Usernames, passwords, credit card details, etc.	Confidential information, business secrets, etc.

SECURITY AWARENESS TRAINING

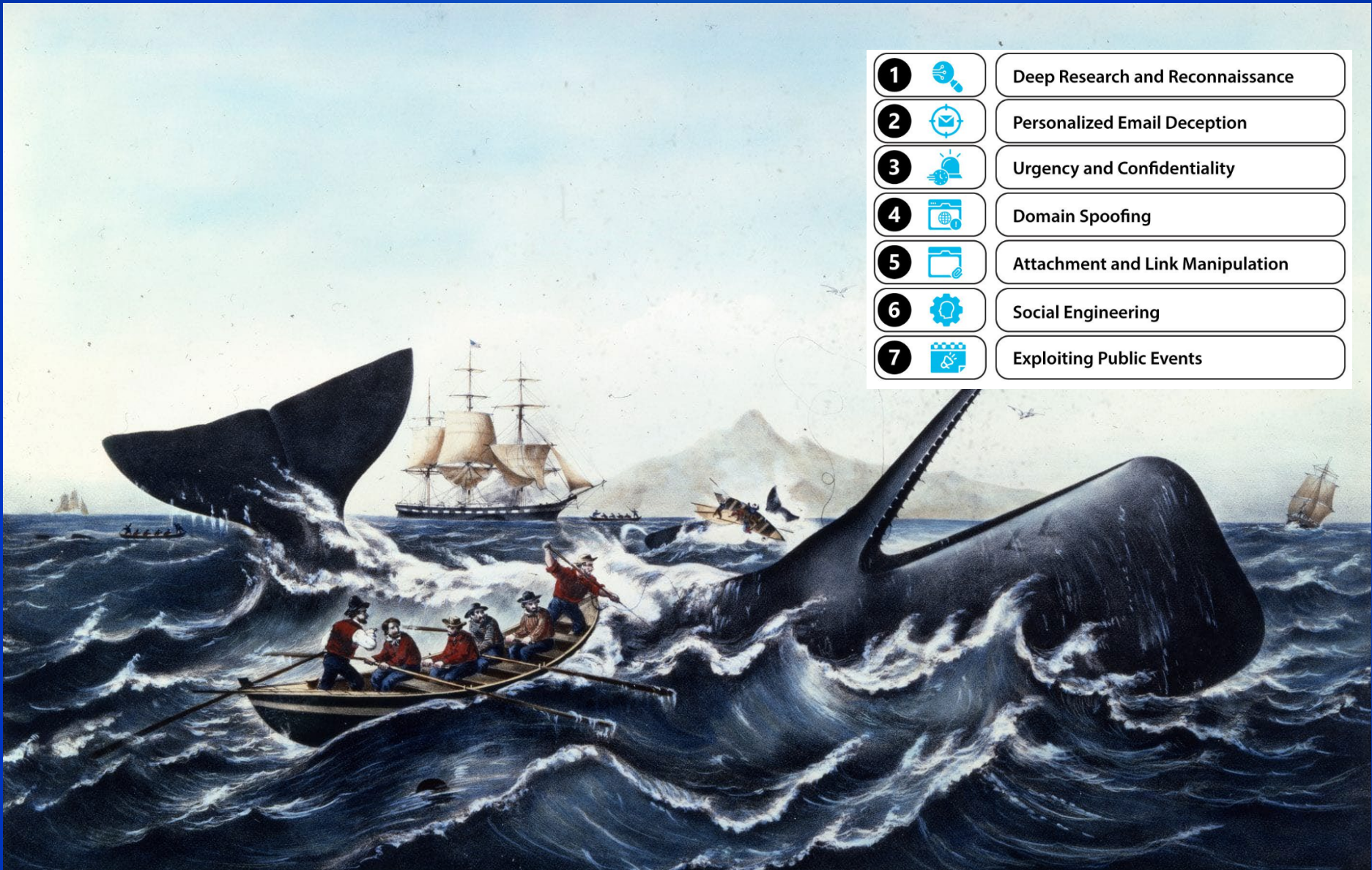
KnowBe4








[Phishing-vs-SpearPhishing.jpg \(1000×1545\)](#)
[\(knowbe4.com\)](#)

**THIS TYPE OF PHISHING ATTACK
- OR IS IT A MAMMALIAN
ATTACK? - TARGETS HIGH-
PROFILE INDIVIDUALS IN AN
ORGANIZATION**

Answer

WHAT IS WHALING?



- 1  Deep Research and Reconnaissance
- 2  Personalized Email Deception
- 3  Urgency and Confidentiality
- 4  Domain Spoofing
- 5  Attachment and Link Manipulation
- 6  Social Engineering
- 7  Exploiting Public Events

<https://www.whalingmuseum.org/learn/research-topics/whaling-history/whales-and-hunting/>



[Whaling Phishing Explained: Protection Strategies - Keepnet Labs](#)

[What is a Whaling Attack? - Check Point Software](#)

**THIS TYPE OF SOCIAL
ENGINEERING ATTACK (PHISH)
USES THE PHONE TO GAIN
PERSONAL AND FINANCIAL
INFORMATION**

Answer

WHAT IS VISHING?



Key Vishing Statistics

- 33% of America's population **fell victim to phone scams** at least once.
- Americans lost around **\$39.5 billion in 2022** and **\$29.8 billion in 2021**.
- The 2019 survey reveals that the **18-22 demographic** recorded the highest awareness of vishing.
- Monthly average spam calls received by Americans **above 65 Years** is estimated to be **50.4 In 2022**.
- Vishing attacks are resurgent and shockingly on the **rise by 550%** in 2022.
- 68.4 million **people lost money to phone scams** in the US in 2022.
- Neighbor spoofing Vishing **grew to 51%** in the US in 2022.



[The Most Alarming Vishing Statistics You Need to Know in 2023 \(techreport.com\)](https://techreport.com)

**THIS TYPE OF ATTACK SENDS AN
SMS TEXT MESSAGE
ATTEMPTING TO STEAL
CRITICAL INFORMATION OR TO
INSTALL MALWARE ON THE
DEVICE.**

Answer

WHAT IS SMISHING?

What to look for

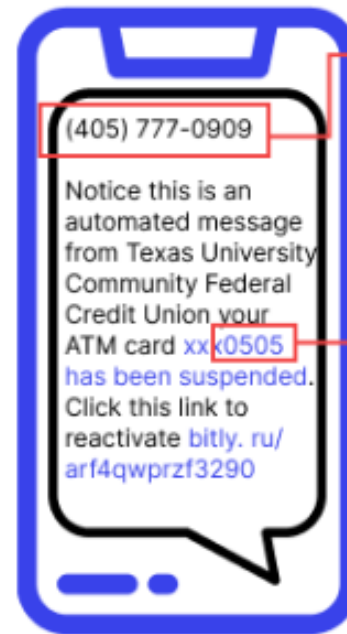
"5555" or another number without a cell phone* is most likely a scammer masking their identity with email and texting services.

Texts can direct you to fake websites that impersonate your accounts and try to steal information.



You are receiving unwanted messages from unknown numbers

Smishers can use part of the number from your debit/credit card to force an answer



What is smishing

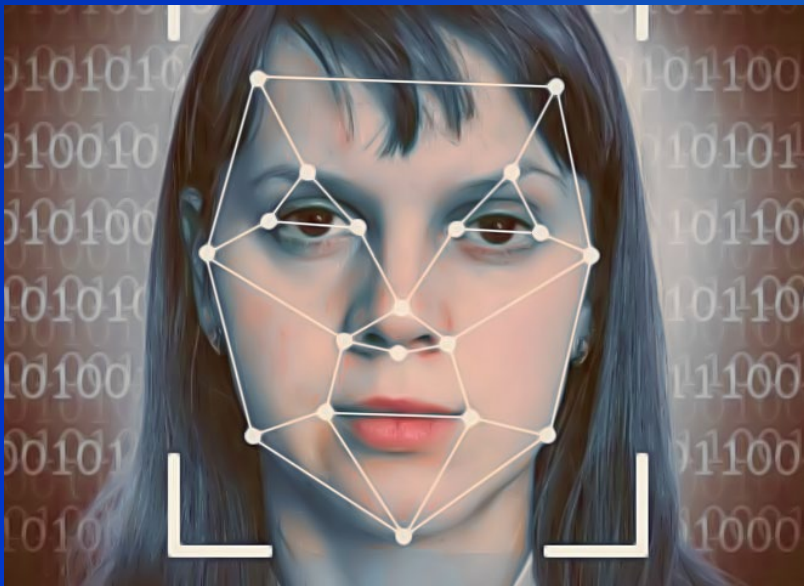
[What is Smishing Attack? Meaning, Definition, Examples \(wallarm.com\)](https://wallarm.com)



COINED IN 2017 THIS TERM
REFERS TO THE RE-CREATION OF
A PERSON'S APPEARANCE OR
VOICE THROUGH ARTIFICIAL
INTELLIGENCE.

Answer

WHAT IS DEEPPFAKE?



How to protect yourself:

1. Limit the amount of data available about yourself.
2. Enable strong privacy settings.
3. Watermark photos.
4. Learn about deepfakes and AI.
5. Use multi-factor authentication.
6. Use long, strong, and unique passwords.
7. Keep your software up to date.
8. Don't take the phishing bait.
9. Report deepfake content.
10. Consult with cybersecurity and data privacy legal experts.

Deepfakes can be:

- Images
- Videos
- Voice recordings
- Live audio



**AN INCORRECT OR FABRICATED
RESPONSE FROM A LARGE
LANGUAGE MODEL OR AI
CHATBOT.**

Answer

WHAT IS AN AI HALLUCINATION?

A 2023 evaluation of chatbots found factual errors present in 46% of their responses.

How to protect yourself:

Always have human oversight

- ✓ Critically evaluate all outputs.
- ✓ Cross check responses with reliable experts.



**THIS INDUSTRY WAS THE MOST
FREQUENTLY TARGETED BY
CYBERCRIMINALS IN 2023,
OUTPACING HEALTHCARE,
GOVERNMENT, AND CRITICAL
INFRASTRUCTURE.**

Answer

WHAT IS THE FINANCE INDUSTRY?



As malicious actors incorporate AI for increasingly sophisticated and more frequent cyberattacks, there is an urgent need for heightened cybersecurity measures to safeguard against these evolving threats.

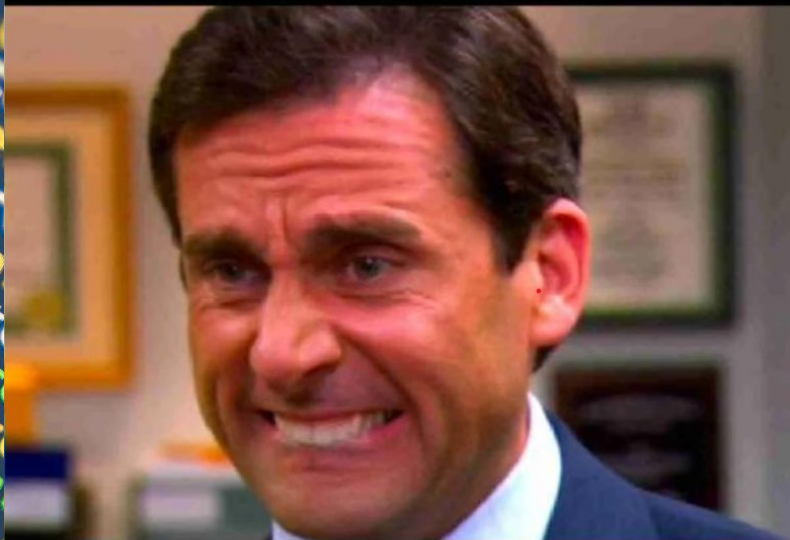


THIS POPULAR CHATTY LARGE LANGUAGE MODEL (LLM) ENABLES CYBERCRIMINALS TO EASILY WRITE MALICIOUS CODE.

Answer

WHAT IS CHATGPT?

WHEN CHATGPT ANSWERS



**YOUR QUESTION BEFORE
YOU EVEN FINISH TYPING IT**







THANK
YOU