The Changing Nature of Cyber Coverage & Cyber Risk

WPPA – 2025 FINANCE & ADMINISTRATION SEMINAR

Lisa McMeekin, Claims Analyst and Eric Swagerty – Member Relations Representative

enduris™
WASHINGTON

THE MISSION

Enduris

To provide financial protection, broad coverage, and risk management services responsive to members' needs.

Providing Reliability In A Risky World

- Get to know the criminals and their motivations
- Get to know the coverage and the underwriting changes
- Get to know the attack types and vulnerabilities
- Get to know how to prevent attacks and build a resilent culture

Yesterday's Cyber Criminal

TODAY'S CYBER CRIMINAL

Meet Vitaly, a cyber security criminal. He refers to himself as a“consultant”.

He is here to help you secure your network.

Vitaly and his friends want to get to know you better.

Insurance Coverage Response

Evolving Coverage

1997 – 1st stand-alone cyber coverage offered

2003 – breach notification law spurs new coverages

2010s – mainstream adoption in every sector

2020s – COVID19 moves many to remote work. Changes the threat

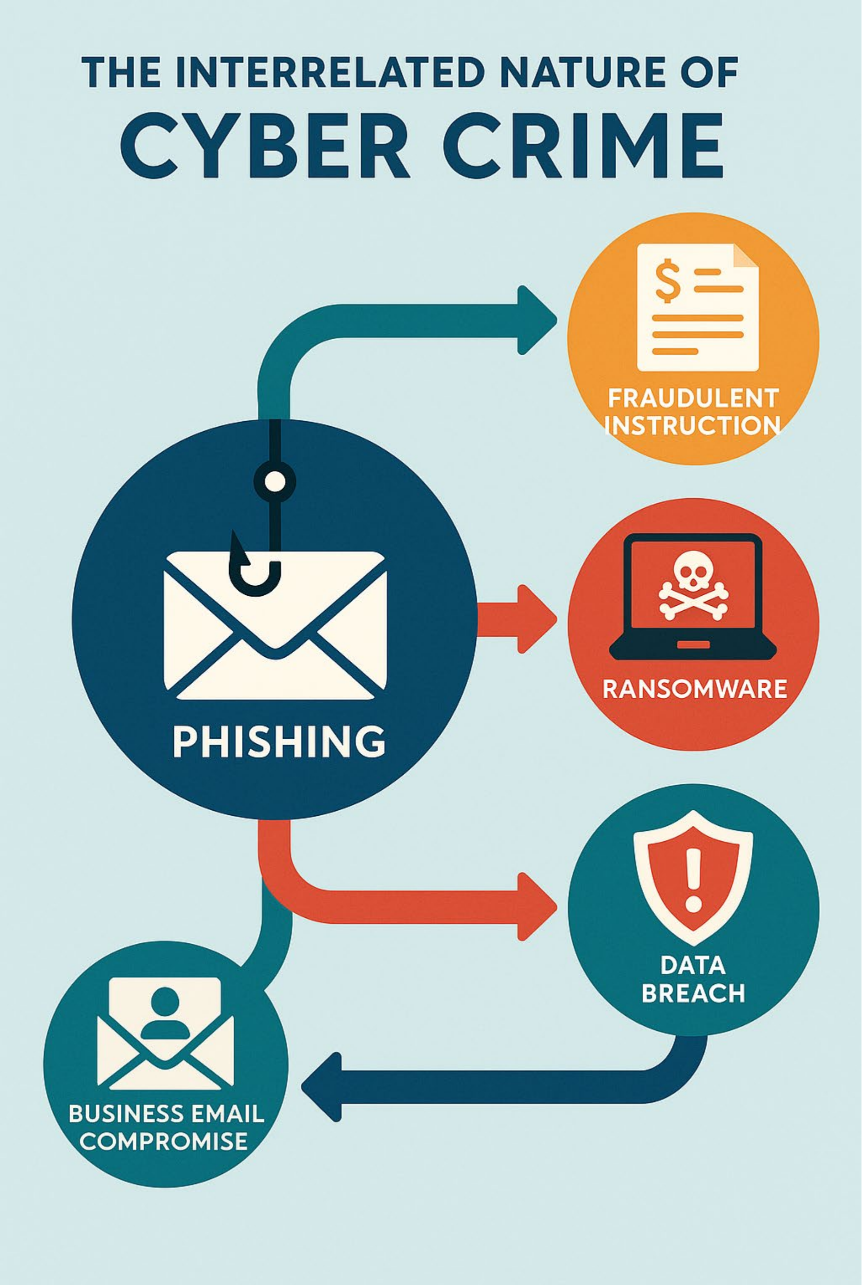
Today – Increasingly stringent underwriting standards and minimum expectations

Changes in Underwriting

Minimum Expectations

1. Multi-factor authentication
2. Anti-phishing attack training
3. Endpoint Protection, Detection and Response
4. Cyber Policies

Interrelated Nature of Cybercrime



WHAT IS CYBERCRIME?

What is "cybercrime"?

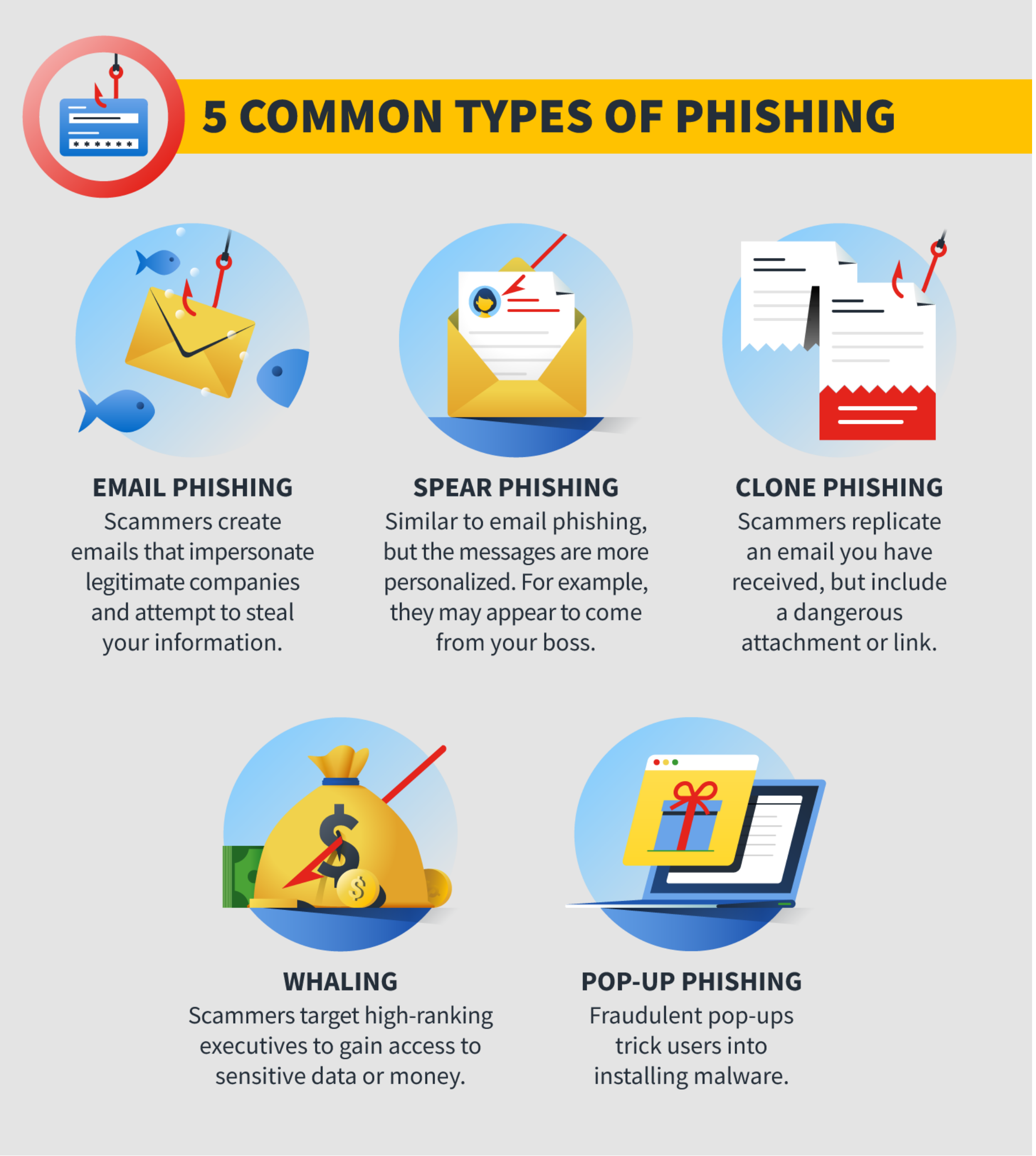
Criminal activities that involve computers, networks, or digital devices.

Involves the breach of a computer system or unauthorized transfer of funds.

Common types of cybercrime leading to cyber claims:

-Phishing scams
-Fraudulent Instruction
-Business Email Compromise (BEC)
-Ransomware Attack
-Data Breach

TYPES OF CYBERCRIME – PHISHING



5 COMMON TYPES OF PHISHING

EMAIL PHISHING
Scammers create emails that impersonate legitimate companies and attempt to steal your information.

SPEAR PHISHING
Similar to email phishing, but the messages are more personalized. For example, they may appear to come from your boss.

CLONE PHISHING
Scammers replicate an email you have received, but include a dangerous attachment or link.

WHALING
Scammers target high-ranking executives to gain access to sensitive data or money.

POP-UP PHISHING
Fraudulent pop-ups trick users into installing malware.

Tips to Identify Phishing Emails

- **Check the Sender's Email Address**: Phishing emails often come from addresses that mimic legitimate ones but have slight variations.
- **Look for Generic Greetings**: Be cautious of emails that start with generic salutations like "Dear User" instead of your actual name.
- **Beware of Urgent Language**: Phishing messages often create a sense of urgency to prompt immediate action without scrutiny.
- **Inspect Links Before Clicking**: Hover over links to see the actual URL. If it looks suspicious or doesn't match the supposed sender, don’t click.
- **Avoid Downloading Unexpected Attachments**: Attachments in unsolicited emails can contain malware.

Types of Cybercrime – Fraudulent Instruction

Fraudulent Instruction

A type of cybercrime where a threat actor impersonates a trusted party (such as an executive, vendor, or client) and issues misleading instructions, often via email or other digital communications, to trick an employee or system into transferring funds or sensitive information.

Relies on **deception and impersonation** rather than technical compromise.

Other Coverage?

Could also be a claim under the Crime policy if a system was not compromised.

Tips to Avoid Fraudulent Instruction

- **Go "Out of Channel":** Do not rely solely on email correspondence. Require additional (human) verification via other means, such as in person or a phone call.
- **Train employees to detect unusual requests:** Prevention is key! Make sure your employees know what to look for.
- **Implement MFA and dual approval for financial transactions**

BEWARE OF FRAUDULENT INSTRUCTION

- VERIFY PAYMENT REQUESTS
- BE CAUTIOUS WITH EMAILS
- CONTACT THE SENDER DIRECTLY

TIPS TO AVOID FRAUDULENT INSTRUCTION

Types of Cybercrime – BEC

Business Email Compromise (BEC)

Business Email Compromise (BEC) is a type of cybercrime in which attackers gain unauthorized access to a business email account and impersonate the email owner to defraud the company, its employees, customers, or partners. BEC attacks are typically targeted and rely heavily on social engineering, rather than sophisticated hacking tools.

The attacker may either *gain access* to a legitimate email account or *spoof* the email address to make it appear as though it comes from a trusted source.

Examples of spoofed email addresses:

lmcmeekin@enduris.us (actual)

lmcmeekln@enduris.us (spoofed)

lrncmeekin@enduris.us (spoofed)

Tips to Avoid BEC

Tips to Avoid Business Email Compromise

- Implement Multi-Factor Authentication (MFA) for email access.
- Conduct regular employee training on phishing and social engineering.
- Use email filtering and threat detection tools.
- Establish strict payment verification protocols (e.g., call-back procedures).

Types of Cybercrime - Ransomware Attack

What is Ransomware?

Ransomware is a type of malicious software (malware) designed to block access to a computer system, network, or data—usually by encrypting files—until a ransom is paid to the attacker.

What happens and how does it happen?

- **Unauthorized Access**: Gaining access to systems through phishing, unpatched vulnerabilities, or Remote Desktop Protocol (RDP) compromise.
- **Data Encryption or Theft**: Locking users out of critical systems and files, and increasingly, **data exfiltration** prior to encryption.
- **Business Disruption**: Rendering essential services and operations inoperable.

Tips to Avoid Ransomware Attacks

🛡 Tips to Avoid Ransomware Attack

- **Network Segmentation**: Limit the spread of malware across systems.
- **Endpoint Detection and Response (EDR)**: Identify and isolate threats early.
- **Patch Management**: Keep all systems updated to prevent known vulnerabilities from being exploited.
- **User Training**: Teach staff how to recognize phishing and suspicious behavior.
- **Backup Strategy**: Maintain offline and regularly tested backups.
- **Incident Response Planning**: Ensure teams are trained and plans are rehearsed.

Types of Cybercrime – Data Breach

Data Breach

Any unauthorized access to confidential, sensitive or protected information release of personal information, known as PII.

A data breach can occur without a cyberattack! It can also include exposure of sensitive information due to Accidental Disclosure or Physical Theft.

Unauthorized access to PII

Personally Identifiable Information includes any combination of:

- Full name
- Social Security Number
- Driver's license or state ID number
- Financial account numbers
- Email addresses linked to identity
- Biometric records
- Health information
- Home address or telephone number

Legal and Regulatory Implications

Organizations may be subject to strict rules for:

- **Notifying affected individuals** within a certain time (e.g., 30 days)
- **Reporting to authorities** (e.g., state attorney general, federal agencies)
- **Mitigation requirements**, such as offering identity theft protection
- **Fines and penalties** for noncompliance

The Process

MITIGATE & REPORT: simultaneously **notify IT Dept**. to secure systems & **Report** to Enduris

- Enduris reports to Cyber Carrier
- Cyber carrier will hold a “scoping call” to make vendor recommendations that **may** include:
    - **Attorneys** (known as Privacy Counsel)
    - **Digital forensic expert** (to determine what happened and why it happened, and if any PII was compromised)
    - **ransom negotiator** (to communicate with the threat actor)
    - **notification vendor or call center** (to notify affected individuals)
    - other services

- Privacy Counsel will provide guidance throughout the process and coordinate vendors and workflows. The attorneys also provide attorney-client privilege, to protect information regarding the forensic investigation.

- Enduris will be involved as needed to make sure your entity’s needs/concerns/questions are addressed and answered.

The Biggest Vulnerability

Q: What is the biggest vulnerability in your cyber network?

A: That would be you.

Why? Because you are so kind and generous.

…and you want to get your job done

Training to Prevent Attack

Training

Q: When is the best time to train for a cyber attack?

A: Immediately before the attack.

Q: When is the second-best time to train?

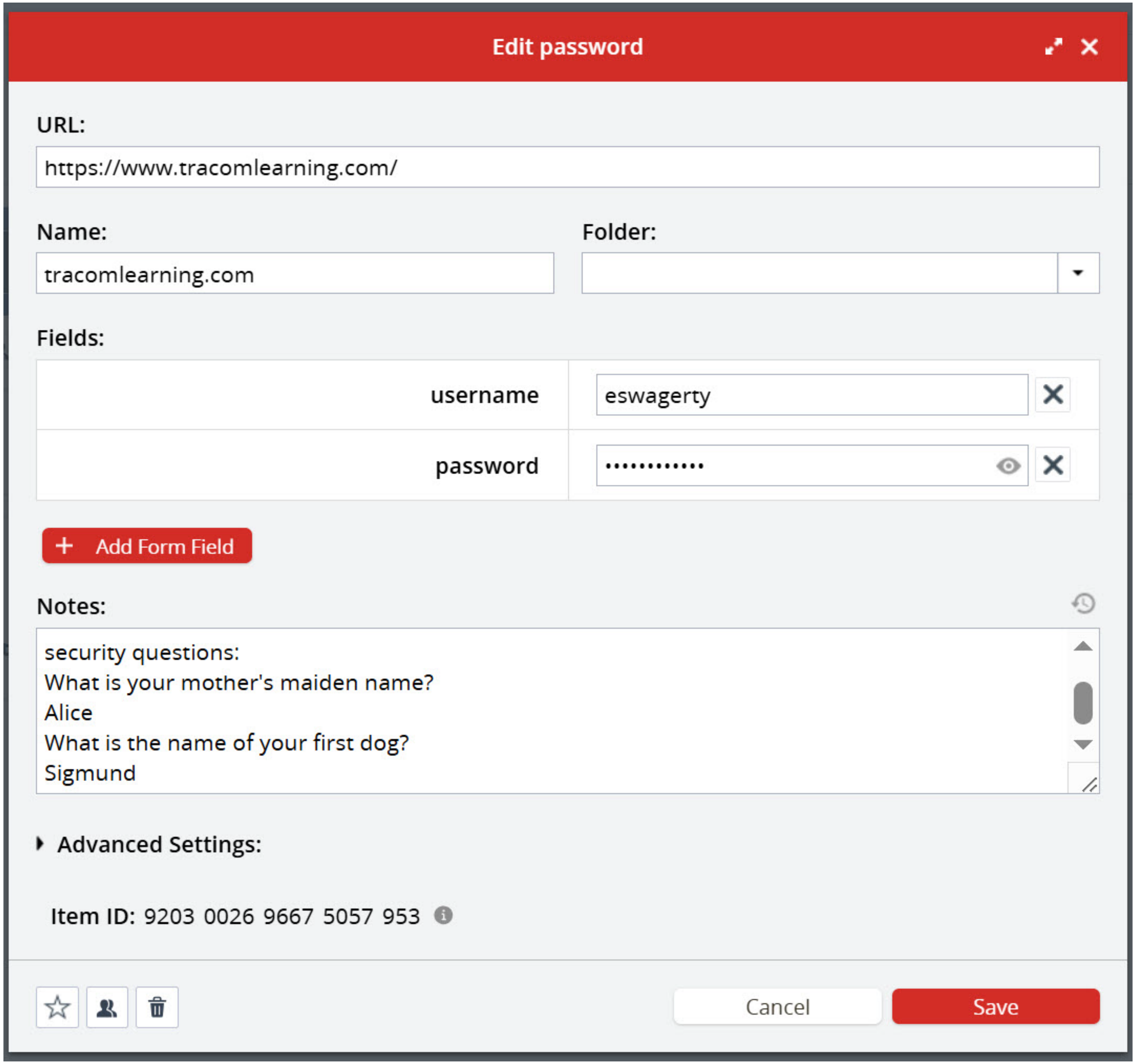
A: Everyday. Seriously.

Reinforce the preventative measures.

enduris WASHINGTON

Something you know, you have, or you are

PASSWORD VAULT



Edit password

URL: https://www.tracomlearning.com/

Name: tracomlearning.com

Folder:

Fields:

username	eswagerty
password	••••••••••••

Notes:

security questions:
What is your mother's maiden name?
Alice
What is the name of your first dog?
Sigmund

Advanced Settings:

Item ID: 9203 0026 9667 5057 953

Zero Trust Policy

Zero Trust

Never trust, always verify.
Reject the unexpected.

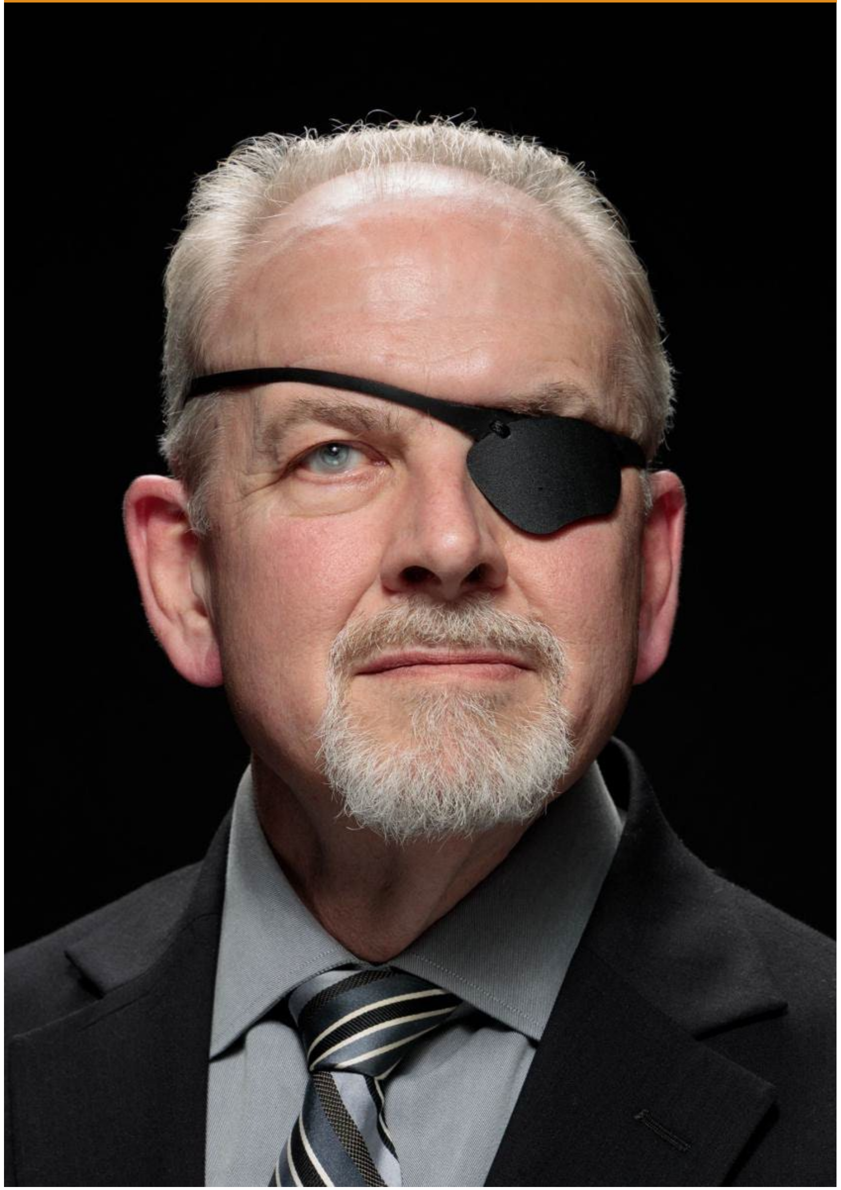
Resources

Use your resources

Out of Channel

Use it as an excuse to call a co-worker, supplier, vendor, customer

Ralph Johnson, WA State CISO



Go Out of Channel

I just called…

Call Me Maybe

Make it fun!

Pick a theme song – habit cueing

Positively reinforce the call when you receive it

Be skeptical

Keep your professional skepticism

Call a known number

Don’t trust your email

Use caution

Better to delay than pay!

IN CLOSING

Q & A

Lisa McMeekin, Claims Analyst

Eric Swagerty

Member Relations Representative

MemberRelations@enduris.us

(800) 462-8418

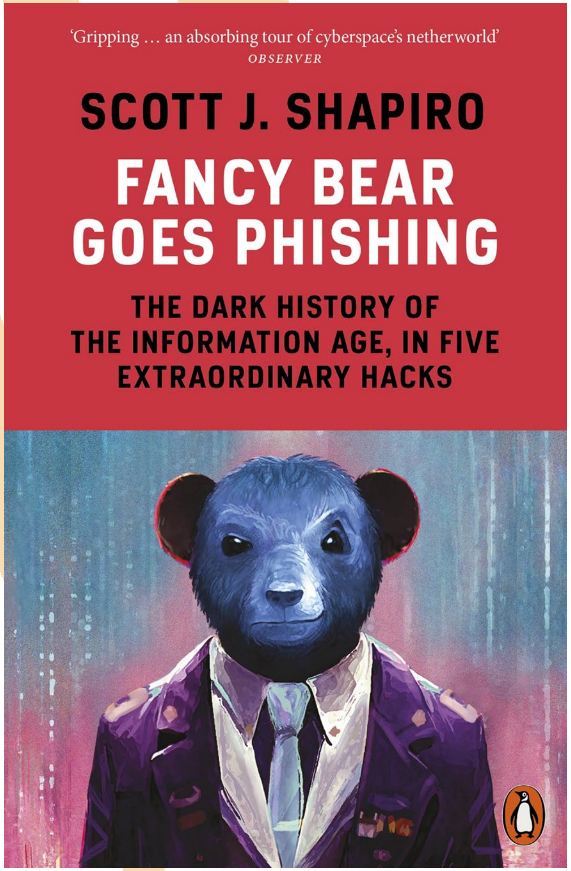
SOURCES AND ATTRIBUTIONS

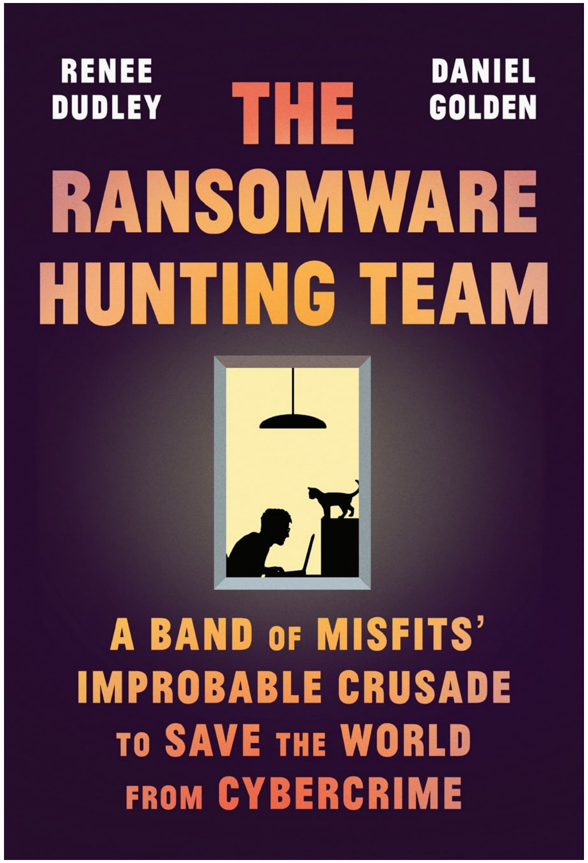
Sources and attributions:

chatGPT and Leonardo.ai for images
Diana Ross concert in Central Park, NY, July 1983

Shapiro, Scott J. *Fancy Bear Goes Phishing: The Dark History of the Information Age, in Five Extraordinary Hacks*. First ed., Farrar, Straus and Giroux, 2023

Dudley, Renee, and Daniel Golden. *The Ransomware Hunting Team: A Band of Misfits' Improbable Crusade to Save the World from Cybercrime*. Farrar, Straus and Giroux, 2022


'Gripping … an absorbing tour of cyberspace's netherworld'
OBSERVER
SCOTT J. SHAPIRO
FANCY BEAR GOES PHISHING
THE DARK HISTORY OF THE INFORMATION AGE, IN FIVE EXTRAORDINARY HACKS


RENEE DUDLEY
DANIEL GOLDEN
THE RANSOMWARE HUNTING TEAM
A BAND OF MISFITS' IMPROBABLE CRUSADE TO SAVE THE WORLD FROM CYBERCRIME