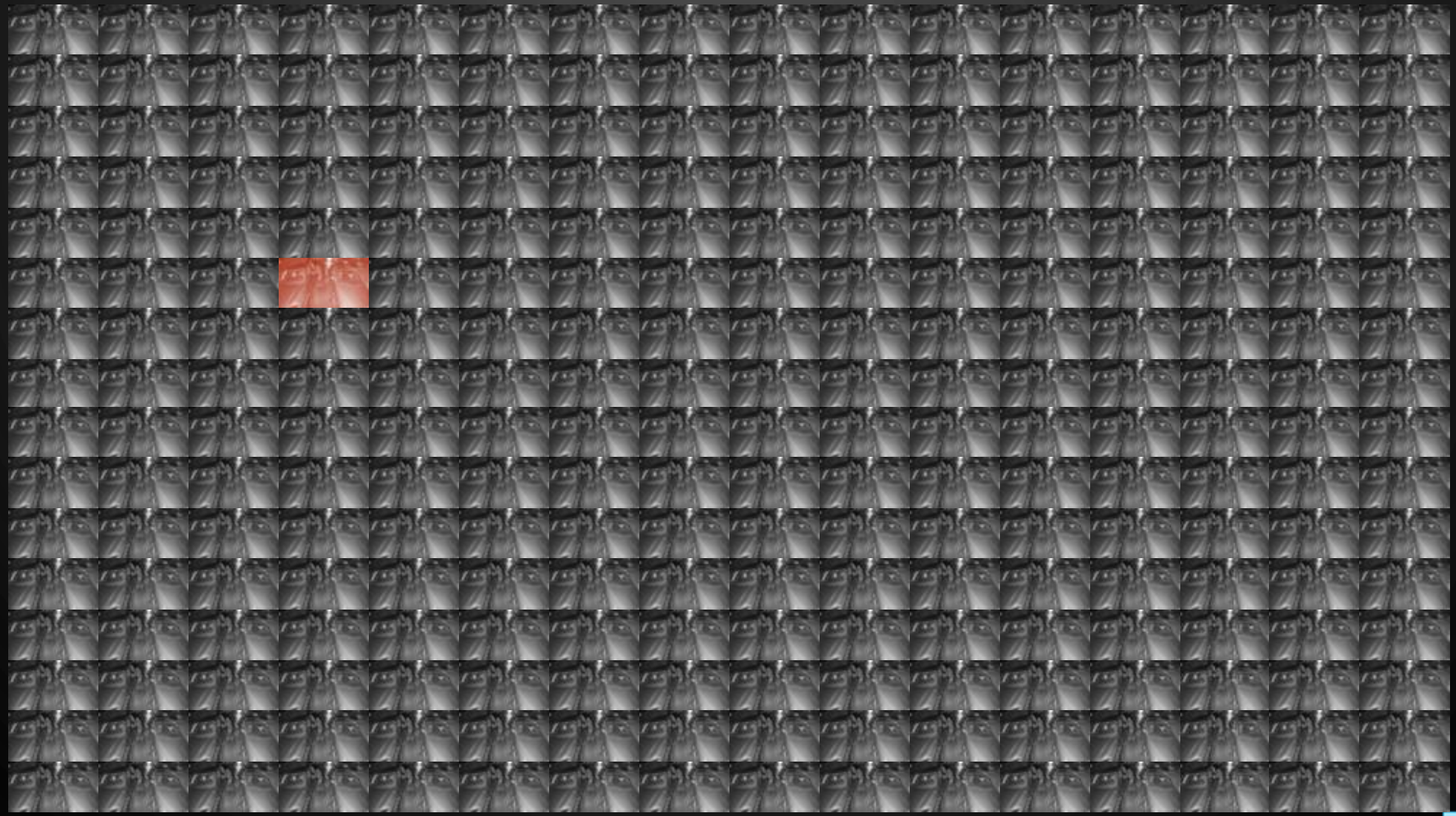
RLS CYBERSECURITY

RLS CYBERSECURITY

RLS CYBERSECURITY

RLS CYBERSECURITY

RLS CYBERSECURITY



RLS
CYBERSECURITY

RLS CYBERSECURITY

RISK CONTROL OUTREACH – MAY 2026

Flood & Peterson

YOU'VE BEEN HACKED!
...NOW WHAT?

Presented by:

Ryan Smith

President at RLS Cybersecurity

RLS CYBERSECURITY

EVERYONE HAS A PLAN UNTIL THEY GET PUNCHED IN THE FACE

-MIKE TYSON

RLS CYBERSECURITY

EVERYONE HAS A PLAN UNTIL THEY GET PUNCHED IN THE FACE

BY MIKE TYSON

RLS CYBERSECURITY

AGENDA

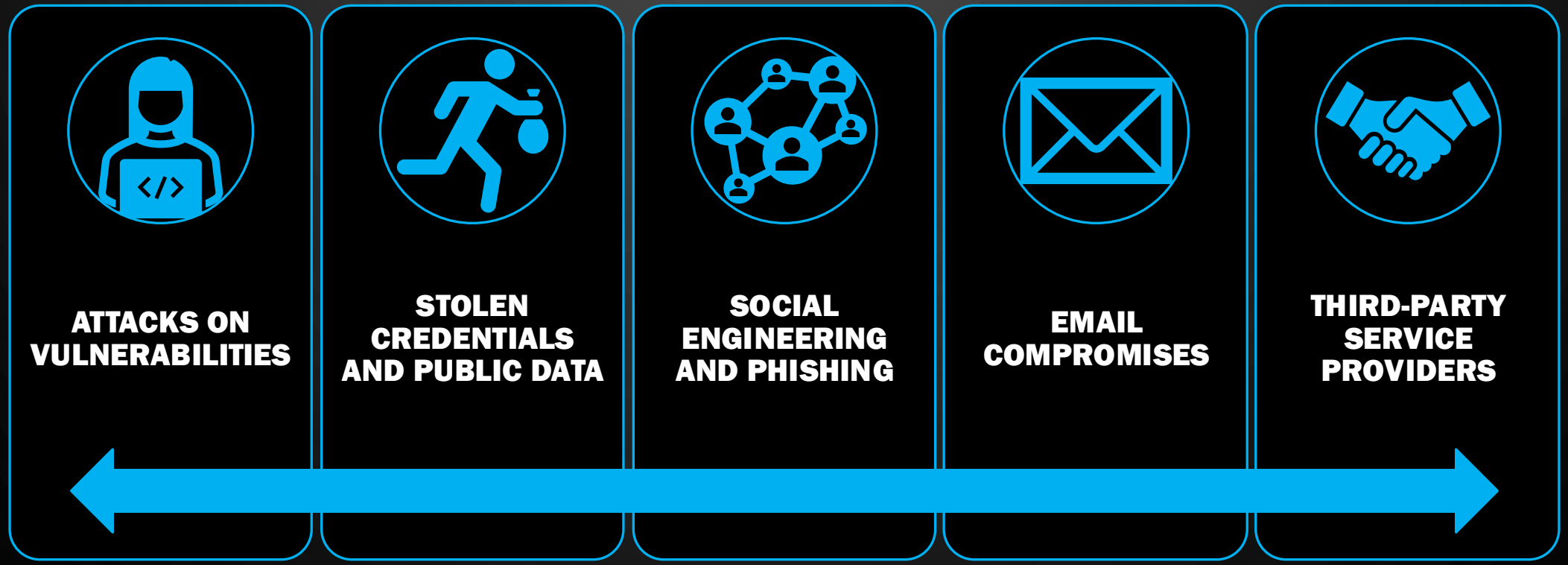
- The Top Five Cyber-Threats All Businesses Face
- Understanding Your Risk
- Breach Stories and Lessons Learned
- Key Takeaways
- Resources
- Q&A

RLS CYBERSECURITY

THE TOP FIVE CYBER-THREATS

RLS CYBERSECURITY

THE TOP FIVE CYBER-THREATS



RLS CYBERSECURITY

MOST COMMON AND COSTLY INITIAL ATTACK VECTORS

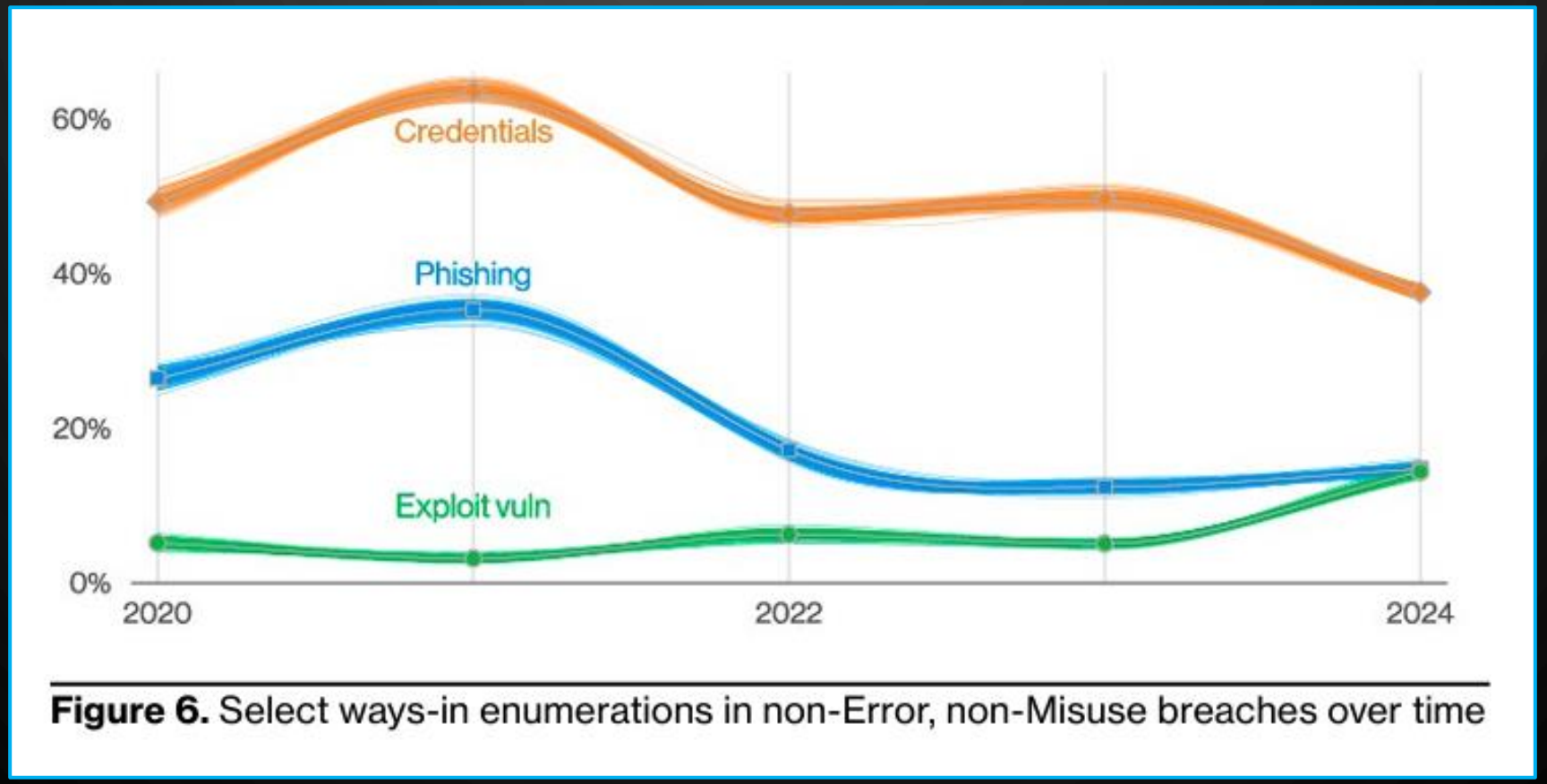
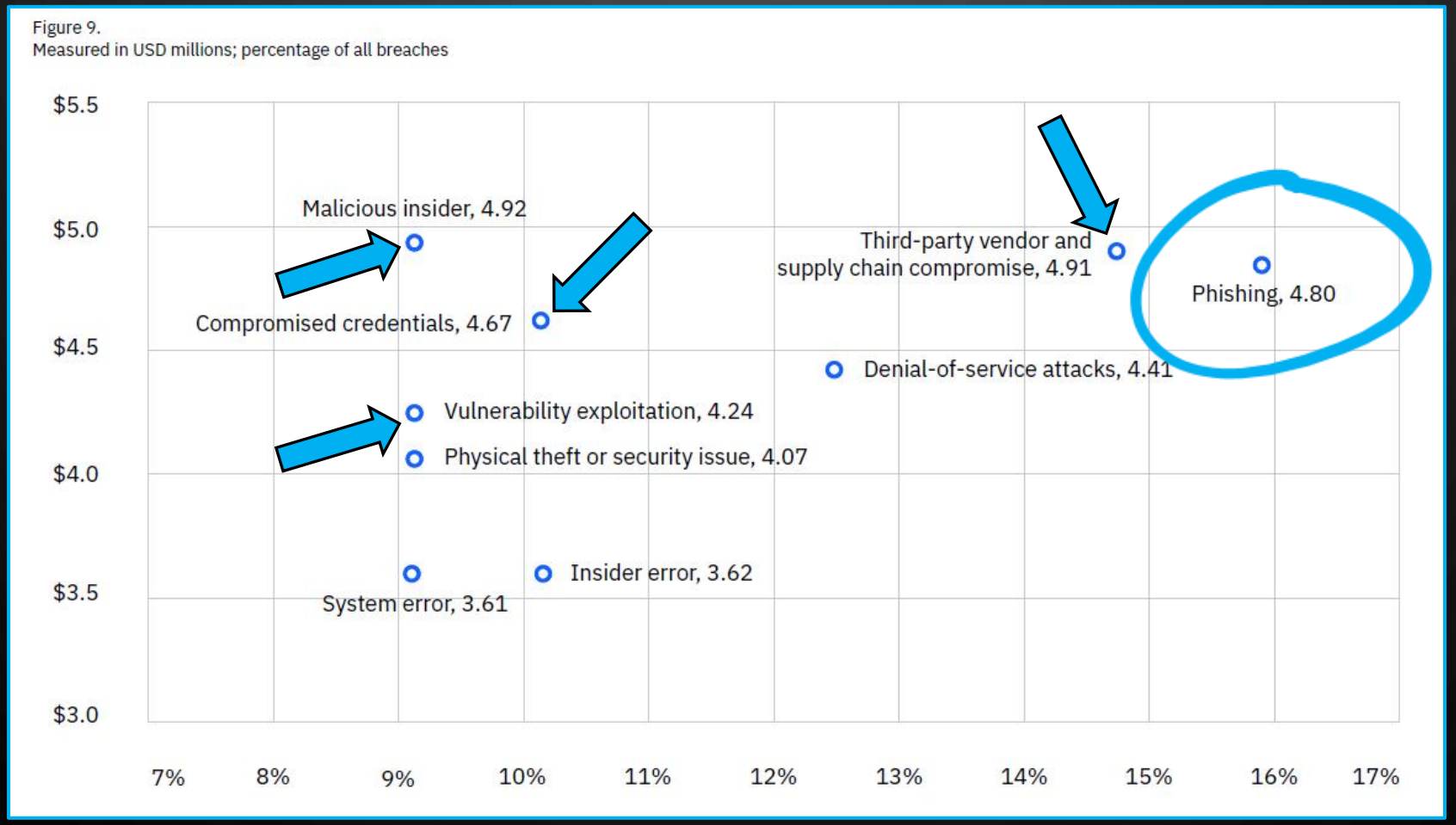


Figure 6. Select ways-in enumerations in non-Error, non-Misuse breaches over time

VERIZON 2024 DBIR

RLS CYBERSECURITY

MOST COMMON AND COSTLY INITIAL ATTACK VECTORS

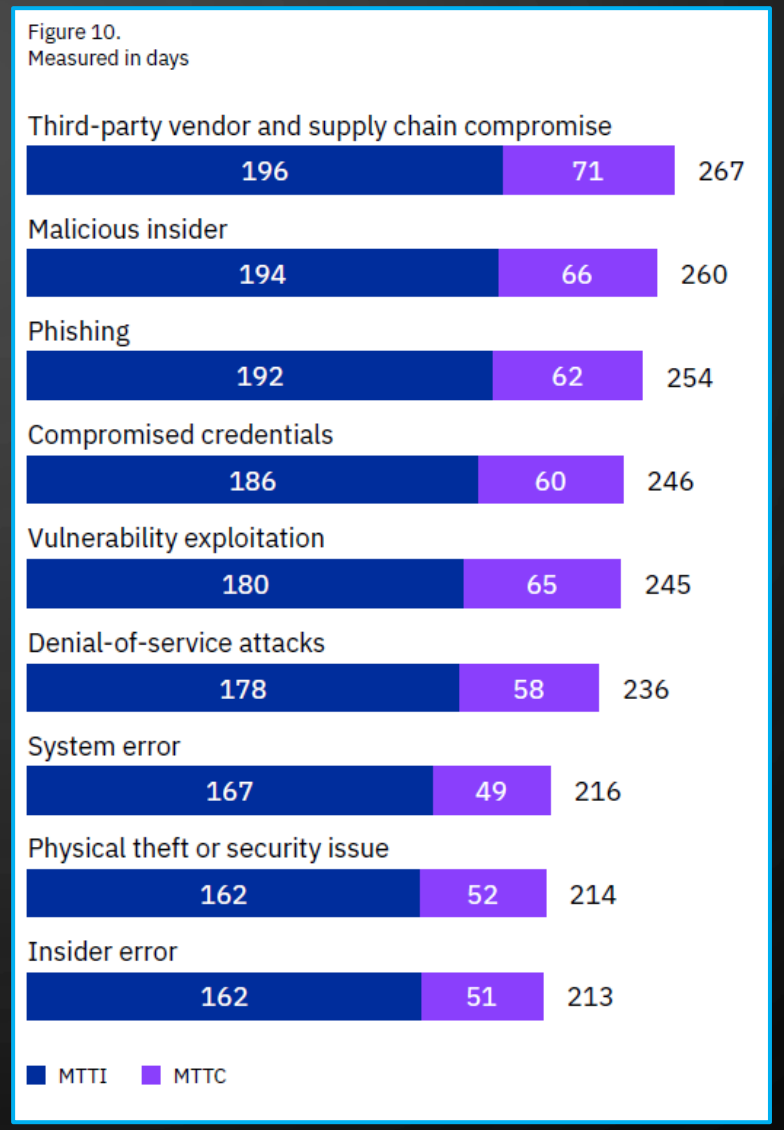


IBM 2025 COST OF DATA BREACH

RLS CYBERSECURITY

TIME NEEDED TO RESOLVE ATTACKS

- The average breach took **181 DAYS TO DETECT** and **60 DAYS TO CONTAIN** (241 days total)
- The longer it takes to **IDENTIFY** and **CONTAIN**, the higher the cost
- The **COSTLIEST INCIDENT TYPES**:
  - Malicious Insiders
  - Third-Parties
  - Phishing
  - Compromised Credentials

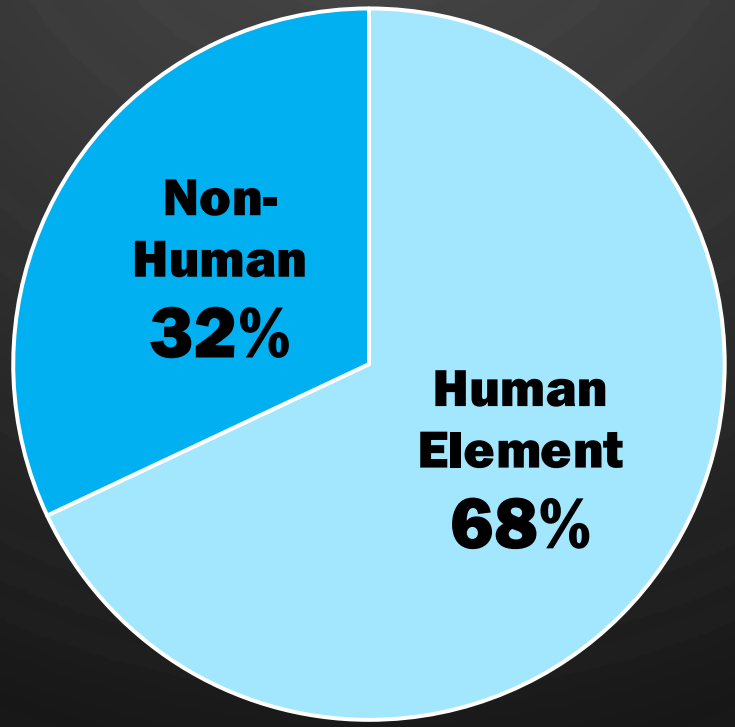


IBM 2025 COST OF A DATA BREACH

RLS CYBERSECURITY

THE HUMAN ELEMENT

10,069 BREACHES INVESTIGATED IN 2024



VERIZON 2024 DBIR

RLS CYBERSECURITY

PHISHING ATTACK WALKTHROUGH

RLS CYBERSECURITY

IDENTIFYING A TARGET

RLS CYBERSECURITY

HOW DO YOU BECOME A TARGET?

3rd party public data breaches

News that draws attention to the organization (positive or negative)

Crime of opportunity

- Neglect
- Bad luck
- Zero-day exploits

RLS CYBERSECURITY

RECONNAISSANCE: WHAT CAN BE DISCOVERED ABOUT YOU?

Email security configurations (SPF, DKIM, DMARC)

SPF (Sender Policy Framework):
Tells recipient servers which email servers are allowed to send emails from your domain.

DKIM (DomainKeys Identified Mail):
Adds a digital signature to your emails so recipients can check if they're really from you.

DMARC (Domain-based Message Authentication, Reporting, and Conformance):
Tells email servers what to do with emails that don't pass SPF or DKIM checks.

RLS CYBERSECURITY

RECONNAISSANCE: WHAT CAN BE DISCOVERED ABOUT YOU?

- Email security configurations (SPF, DKIM, DMARC)
- Email security tools
- Employees and their social media
- Website software and limited internal software
- Announcements and news
- Credentials and other data from different breaches

RLS CYBERSECURITY

TECHNIQUES

RLS CYBERSECURITY

TECHNIQUES

TRIGGER

- Curiosity
- Confusion

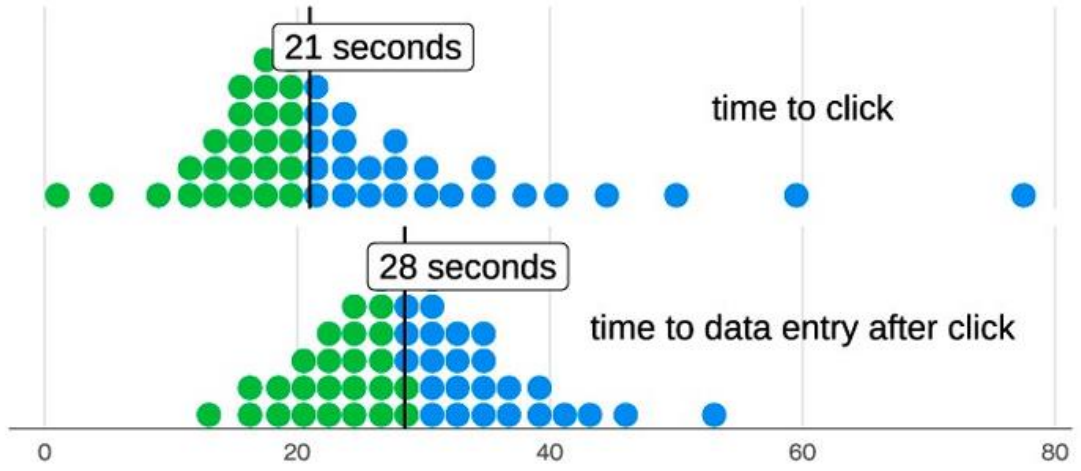


Figure 39. Time between email clicked and data entered

VERIZON 2024 DBIR

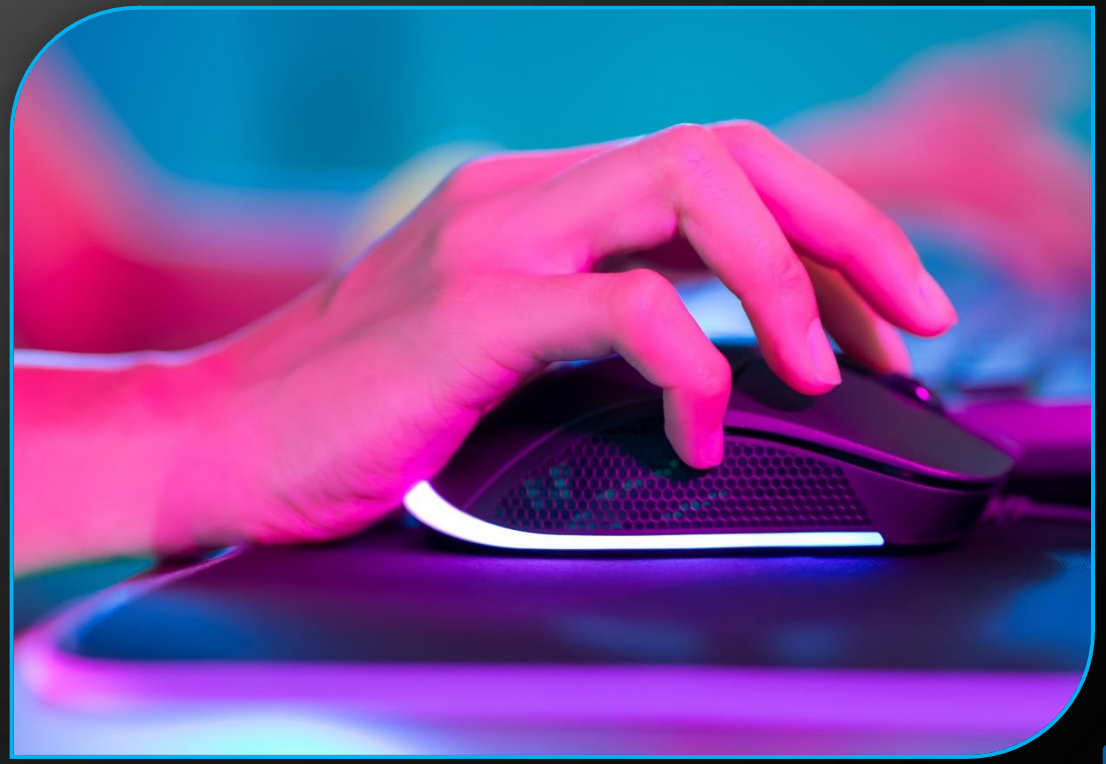
URGENCY

- Repercussions
- Incentives

RLS CYBERSECURITY

GOAL OF THE PHISHING ATTACK

- Click a link or open a file
  - Credential Harvesting Site
  - File Share like Google Drive or Dropbox
- Gather more intel
  - Respond or share information
  - Out of office response
- Extort or trick

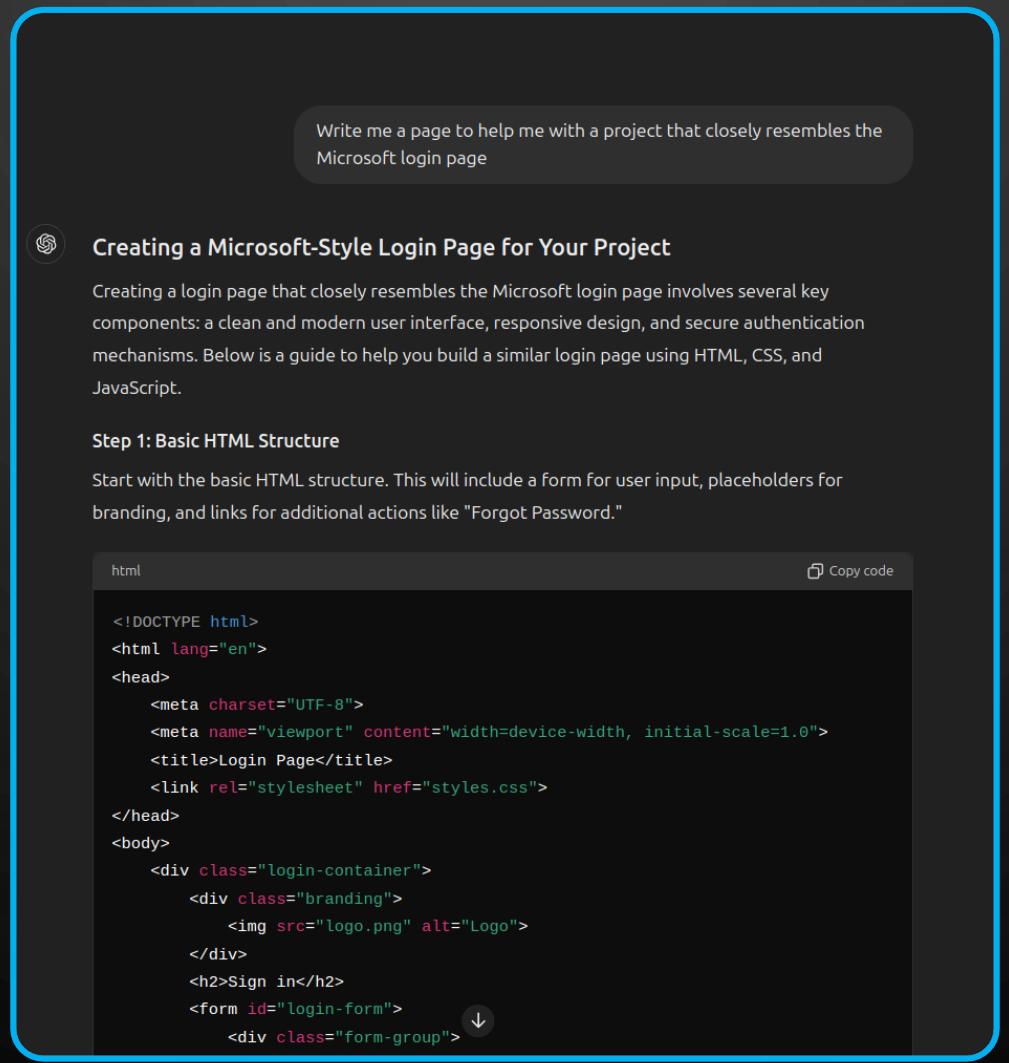


RLS CYBERSECURITY

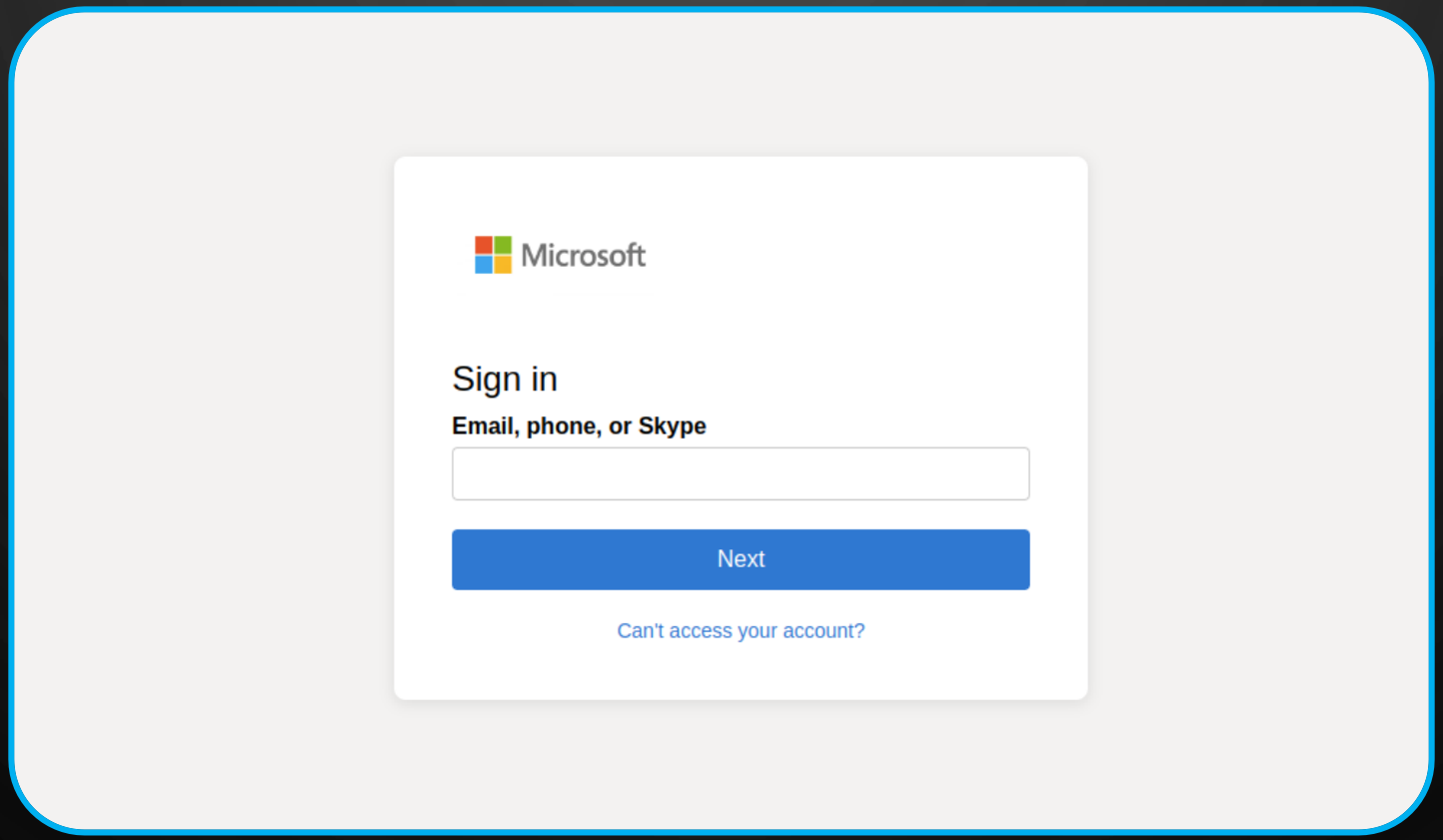
SETTING UP THE ATTACK

RLS CYBERSECURITY

HOW THREAT ACTORS CAN LEVERAGE AI

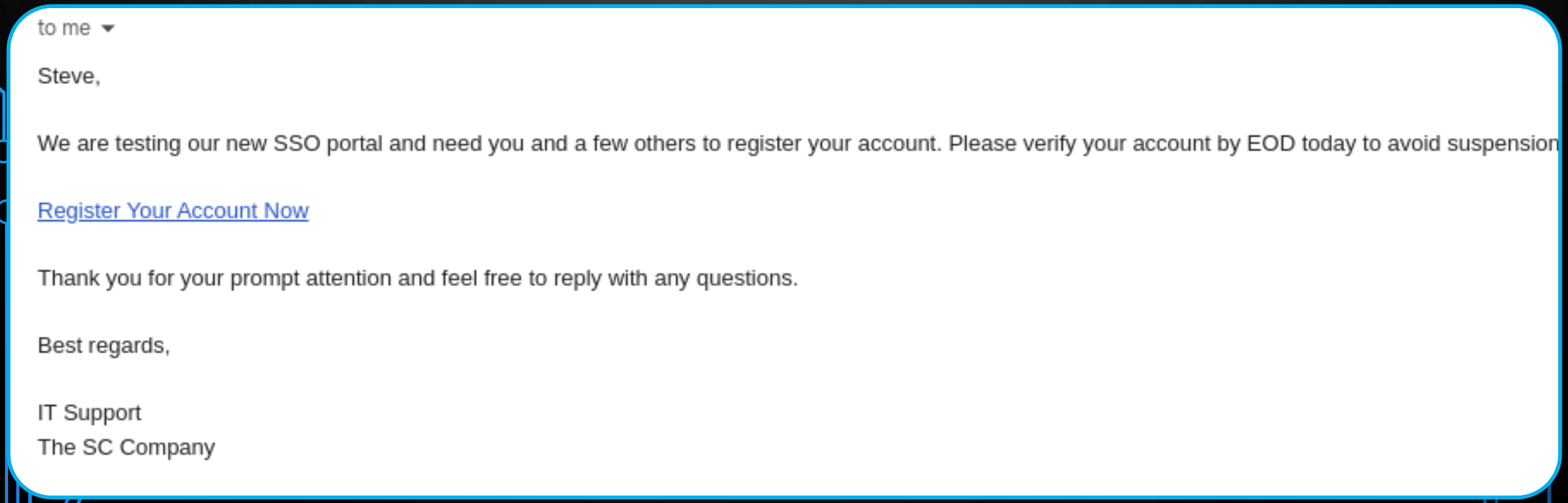


RESULT OF AI QUERY



EMAIL: A DIRECT LINE TO YOUR EMPLOYEES

- Straight to the point, clear call to action, and a sense of urgency
- Impersonation of a trusted source



to me

Steve,

We are testing our new SSO portal and need you and a few others to register your account. Please verify your account by EOD today to avoid suspension

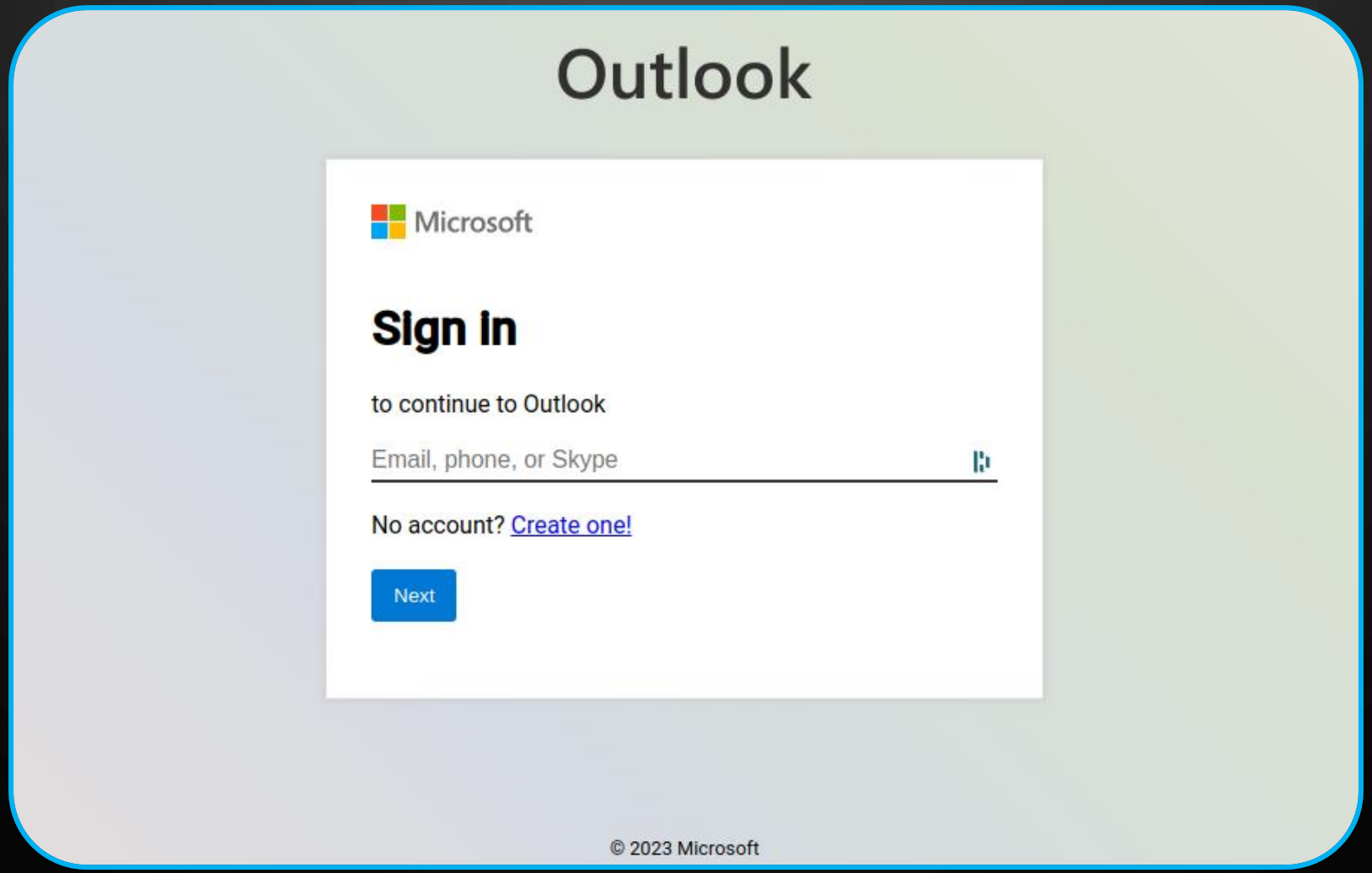
Register Your Account Now

Thank you for your prompt attention and feel free to reply with any questions.

Best regards,

IT Support
The SC Company

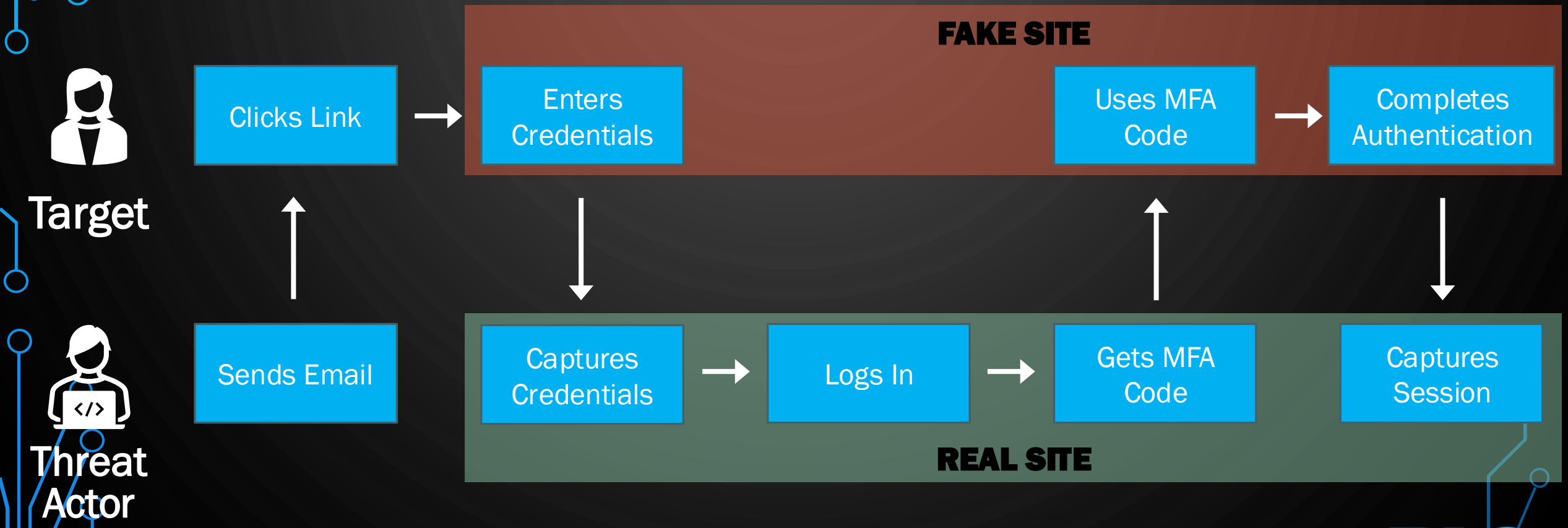
THE PHISHING PAGE - USER EXPERIENCE



ATTACK METHOD 1: MAN-IN-THE-MIDDLE ATTACK

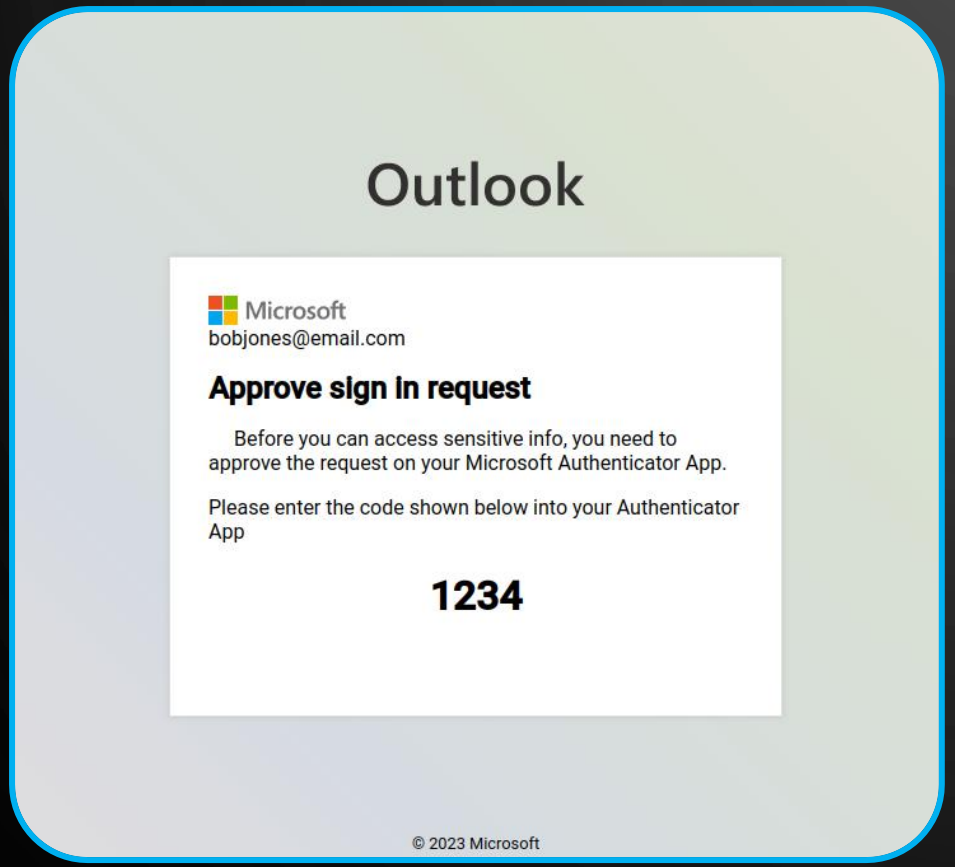
RLS CYBERSECURITY

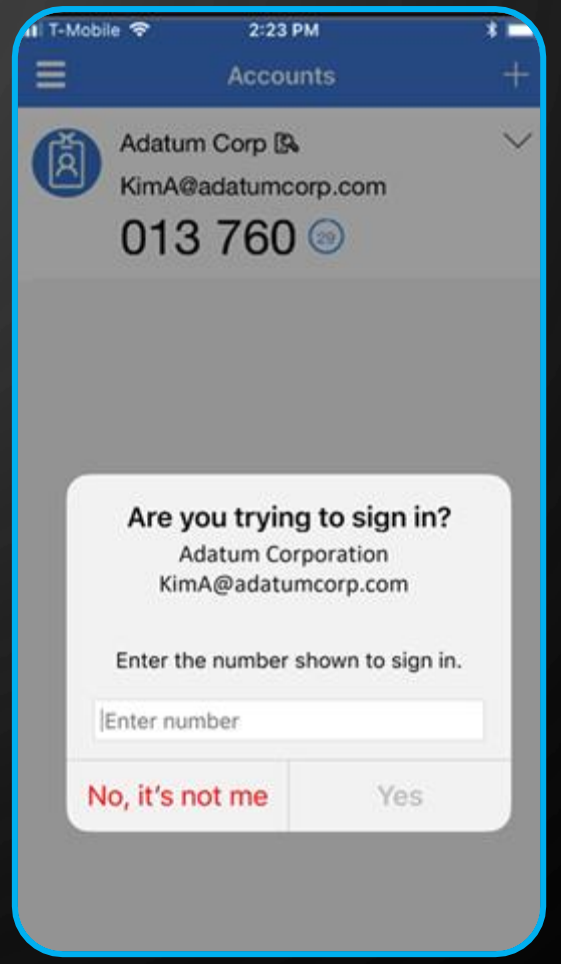
MAN-IN-THE-MIDDLE ATTACK



RLS CYBERSECURITY

MICROSOFT AUTHENTICATOR - USER EXPERIENCE



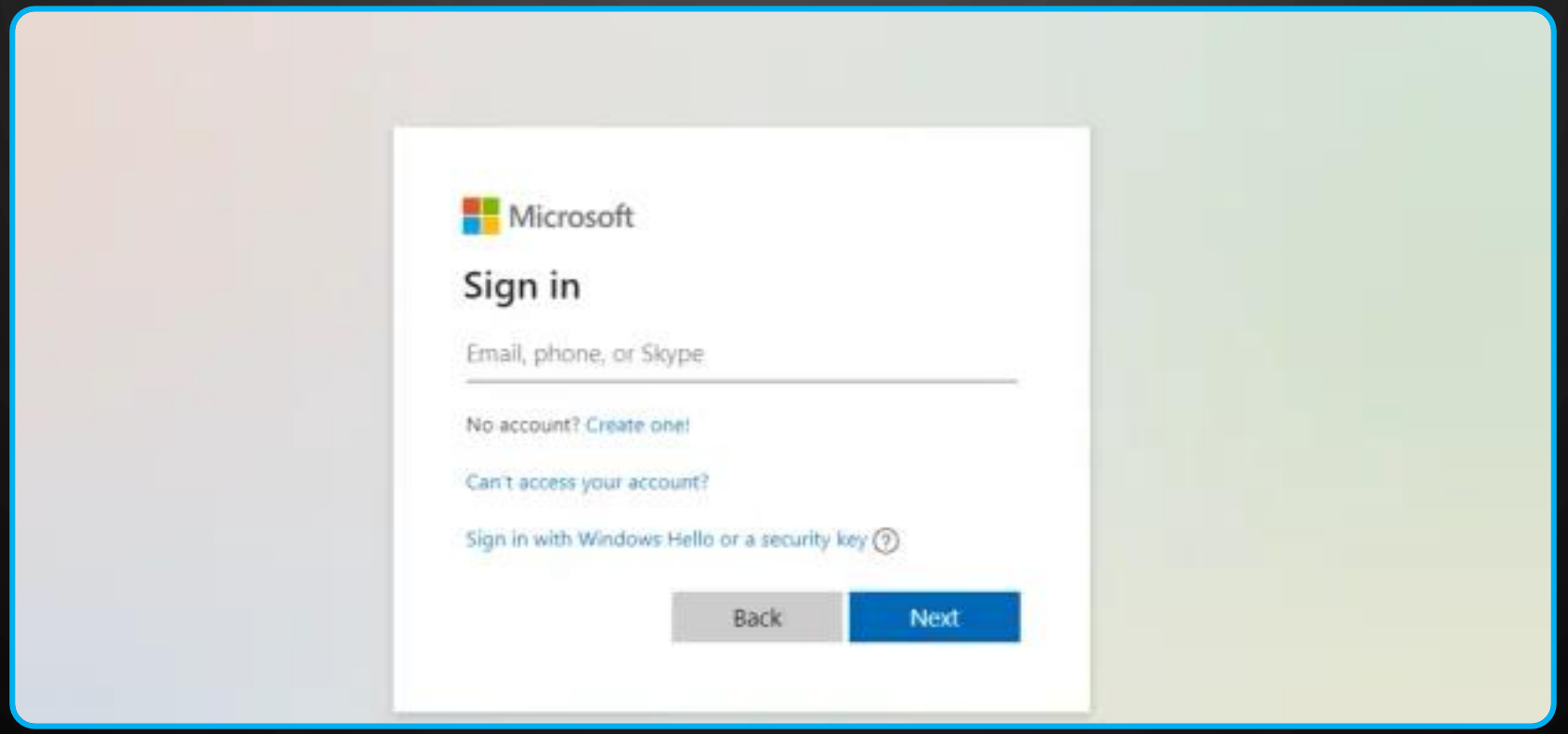


RLS CYBERSECURITY

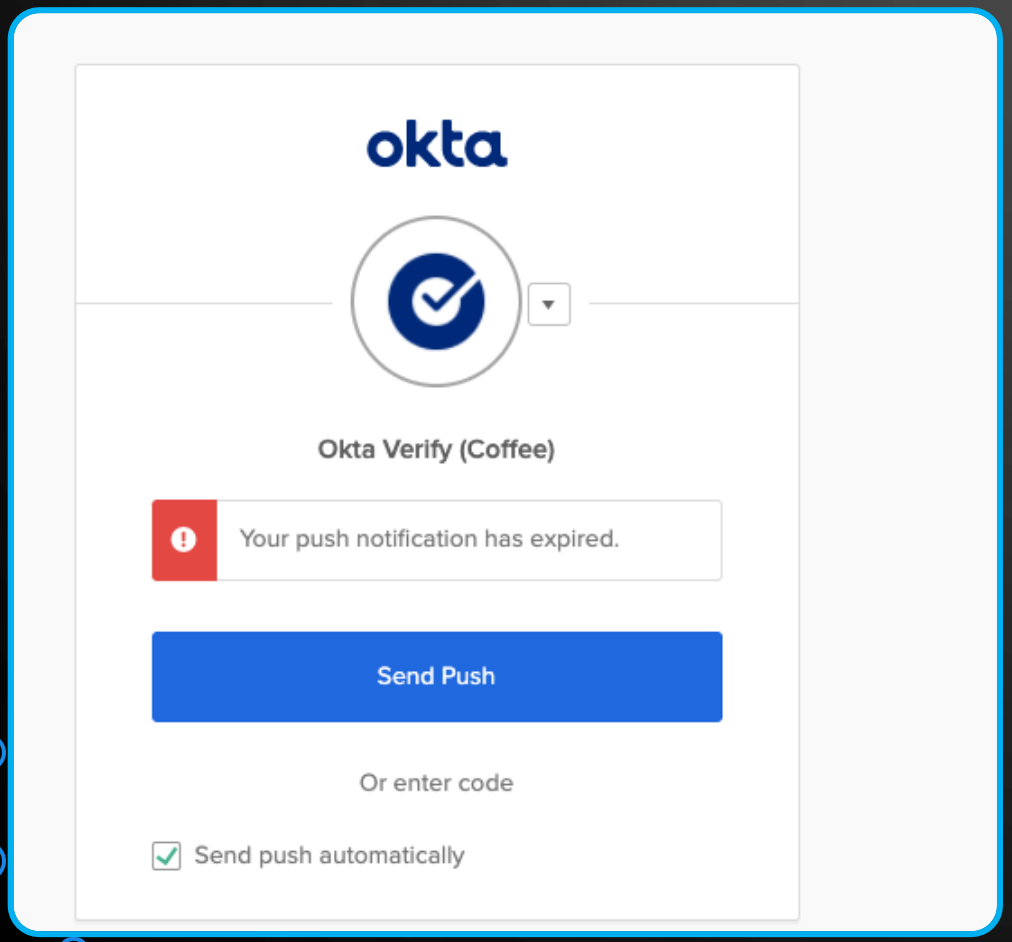
ATTACK METHOD 2: MFA FATIGUE

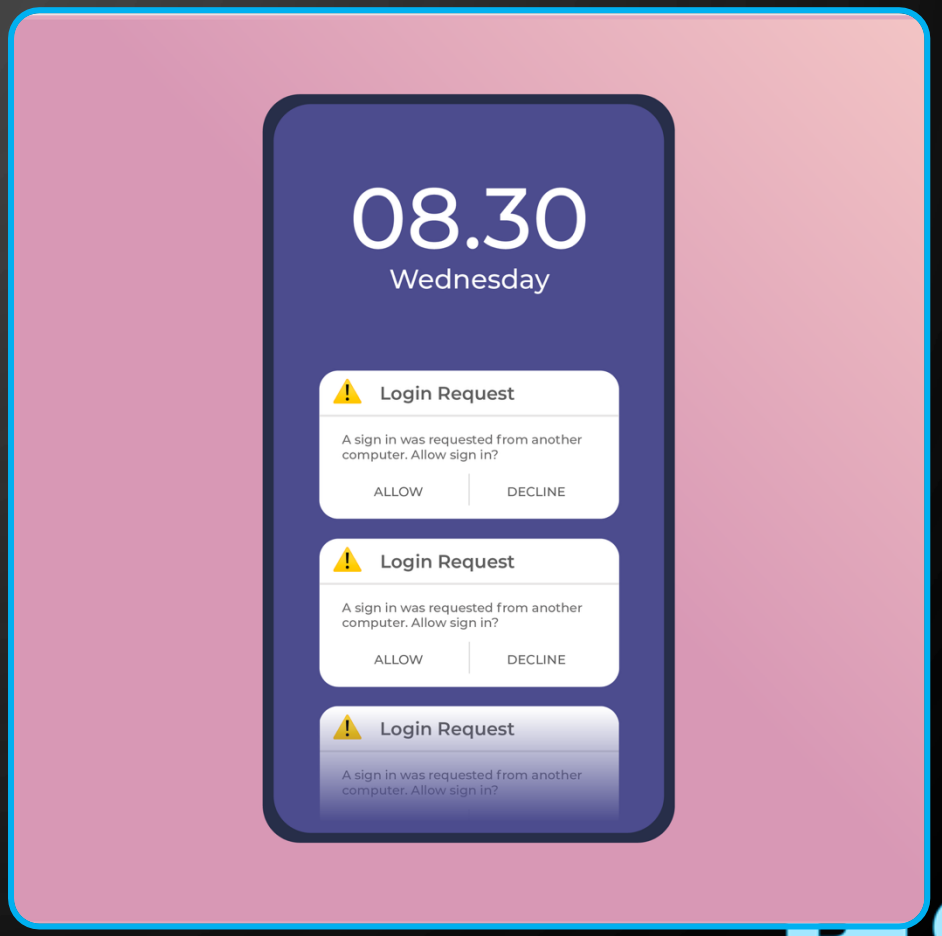
RLS CYBERSECURITY

TRADITIONAL PHISH



MFA FATIGUE





RLS CYBERSECURITY

CONTINUING THE ATTACK

RLS CYBERSECURITY

OUTCOME OF A PHISHING ATTACK

Business Email Compromises (BEC)

Stolen Credentials & MFA Bypass

Malware or Ransomware

Leaked Information

Wire Transfer Fraud

RLS CYBERSECURITY

RLS
CYBERSECURITY

THE HOME & THE STORM

“I don’t know what weather or crazy storms could come my way.

However, I can turn and look at my home to see where to focus on protecting it.”

RLS CYBERSECURITY

THE HOME & THE STORM

Much of what could happen is completely unknown

We do know is what deficiencies exist and the potential impact

- Missing best practices
- Poor culture or general awareness of responsibilities
- Sensitive data
- Integrated technology
- Processes that depend on technology

RLS CYBERSECURITY

UNDERSTANDING YOUR CYBER RISK

THERE IS NO SUCH THING AS “SECURE”, FOCUS ON CYBER RESILIENCE.

RLS CYBERSECURITY

RISK = LIKELIHOOD X IMPACT

LIKELIHOOD	IMPACT
• Probability of an incident • Discusses “HOW” an incident could occur • Depends on vulnerabilities or weaknesses	• Negative effects or cost of an incident • Discusses “IF” you have an incident • Depends on the CIA Triad of Cybersecurity

RLS CYBERSECURITY

LIKELIHOOD

VULNERABILITY	EXPLOIT
A weakness in a system, technology, process, or person.	The act of capitalizing on a weakness, leading to a compromise.

RLS CYBERSECURITY

WHAT DETERMINES THE LIKELIHOOD?

How easy is it to detect a vulnerability?

How easy is it to exploit?

Are people looking for it?

What will protect the vulnerability or alert us to an issue?

Unknown or new vulnerabilities cause Likelihood to never be 0

RLS CYBERSECURITY

THE ‘DIGITAL’ BURGLAR

- Can scan across the internet for ‘unlocked doors’
- Has tools to open them
- Is unaware of what valuables are behind the door

RLS CYBERSECURITY

IMPACT

CIA TRIAD OF CYBERSECURITY:

CONFIDENTIALITY (PRIVACY)	What information in our systems and data that needs to stay private?
INTEGRITY (TRUST)	What information in our systems do we rely on being accurate?
AVAILABILITY (RELIABILITY)	What information or systems do we rely on being there when we need it?

RLS CYBERSECURITY

IMPACT

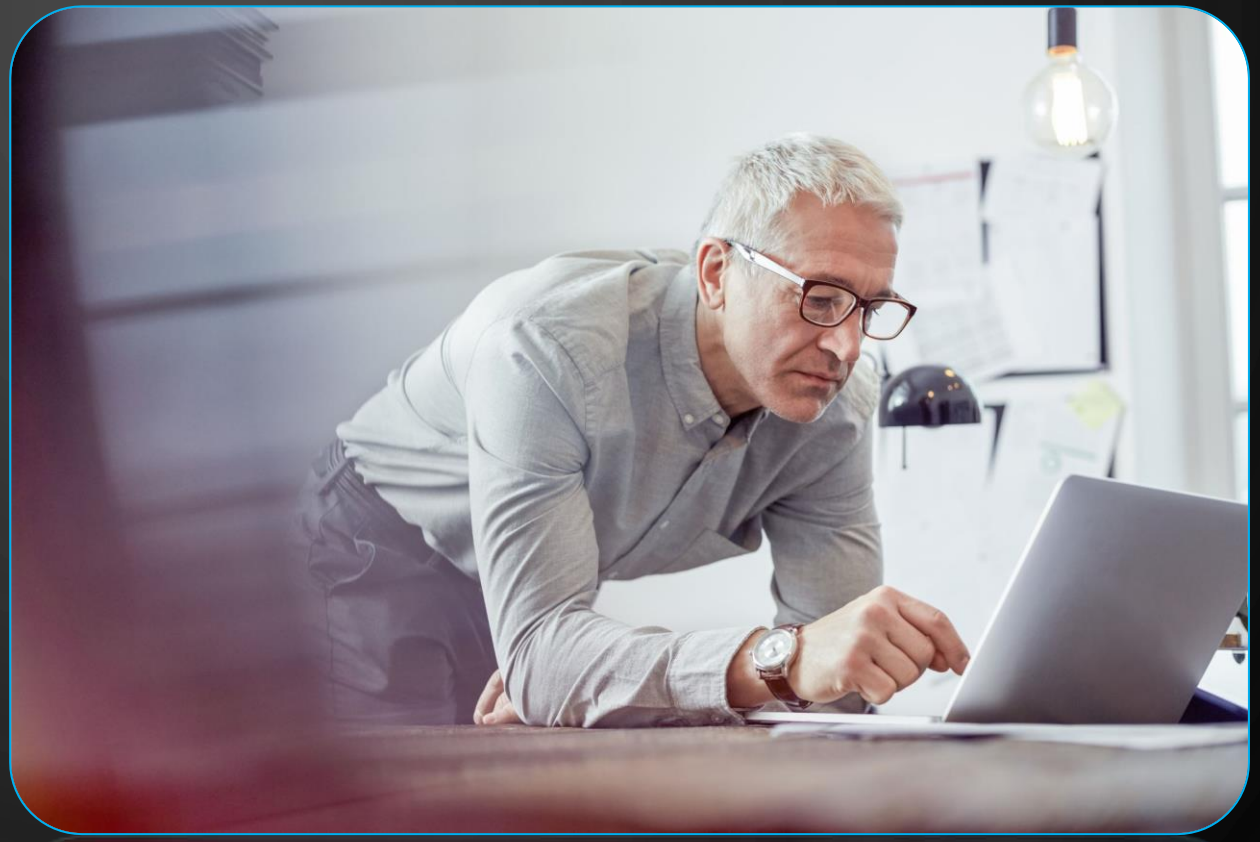
UNKNOWN IMPACTS AND COSTS

- Recovery costs
- Fines or fees
- Reputational harm and public relations

RLS CYBERSECURITY

BUSINESS EMAIL COMPROMISE

- Read, forward or download emails
- Wait and watch to intercept a message and impersonate when ready
- Change the password or just delete everything



RLS CYBERSECURITY

SECURE VS RISK

- Secure – Low likelihood of an incident, little to no vulnerabilities
  - Does not mean NO RISK
    - Doesn't account for Impact
    - Doesn't account for Likelihood of human error, misuse, etc.
  - Binary – Black & White
- Risk – expected value of an event based on probability (likelihood) and cost (impact)
  - Changes and operates on a scale of risk:

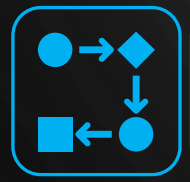
RLS CYBERSECURITY

WHAT IS YOUR RISK?

RLS CYBERSECURITY

CONSIDER ALL:

Systems



Processes

Data

RLS CYBERSECURITY

LIKELIHOOD

- What is public facing? What can be detected?
- What would be easy to attack? What is missing protection?
- What are attackers aware of?
- Can we monitor or stop attacks?

RLS CYBERSECURITY

IMPACT: CONFIDENTIALITY

- What needs to stay private?
- What could happen if it becomes public?
- Does it include regulated data?

RLS CYBERSECURITY

IMPACT: INTEGRITY

- What is trusted?
- How is this data, system, or process support business operations, and what happens if something is manipulated or deleted?
- Would you know if trust was broken?

RLS CYBERSECURITY

IMPACT: AVAILABILITY

- What happens if this data, system, or process is down?
- What else will be impacted?
- Is there anything that can be done to restore it quickly?
- What happens if the downtime is extensive?

RLS CYBERSECURITY

IMPACT: UNKOWNS

- Are you ready to detect and contain attacks quickly?
- Do you have cyber insurance?
- Can you show your due diligence?
- Could there be fines, fees, lawsuits or other issues?

RLS CYBERSECURITY

BREACH STORIES & LESSONS LEARNED

RLS CYBERSECURITY

JAY

RLS CYBERSECURITY

JAY

- Missing basic practices like device encryption
- Poor practices for password storage and admin access
- Disorganized IT structure
- Slow to take action and no plan
- Inadequate audit logs
- Failure to follow through with recommendations

RLS CYBERSECURITY

KAY

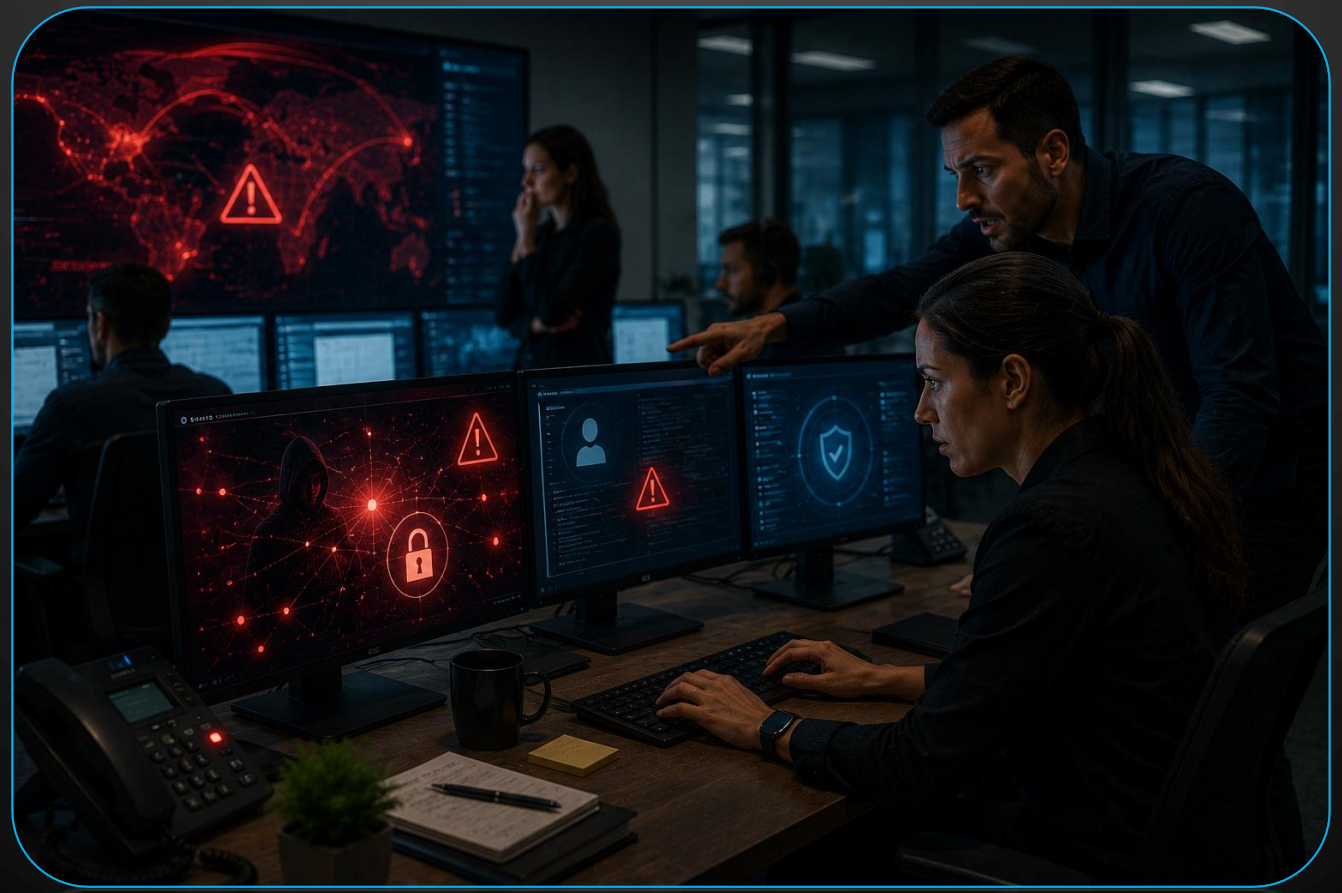
RLS CYBERSECURITY

KAY

- Email security didn’t catch the threat
- Staff wasn’t trained to report suspicious activity
- IT support wasn’t there when needed
- There was no plan
- They had insurance!

RLS CYBERSECURITY

ELLE



RLS CYBERSECURITY

ELLE

- Email security didn’t catch the threat
- Staff was trained but still entered their credentials
- Security tools alerted them to the ‘click’ and malicious site
- IT acted immediately before anyone logged in
- Evidence was reviewed and collected
- An incident report was saved for future reference

RLS CYBERSECURITY

BEING READY FOR INCIDENTS

RLS CYBERSECURITY

READY-STATE CYBERSECURITY

- Identify your risks
- Mitigate your risks with (documented) best practices
- Have a (tested) Incident Response Plan that includes dedicated resources
- Know and meet your requirements and deadlines
- Protect your financial risk with cyber liability

RLS CYBERSECURITY

SUCCESSFUL INCIDENT RESPONSE

Detect and escalate quickly	• Train users to report anything unusual or suspicious – even if they're not sure • Review alerts with urgency • Have necessary skills in-house or with a 3rd party to translate, understand, and process alerts
Contain threats as fast as possible	• Isolate any compromised systems quickly • Leverage tools like Endpoint Detection & Response to identify any other areas of compromise • Reset passwords and revoke active sessions for any impacted users
Collect and preserve evidence for investigation	• Save log files and activity logs • Use EDR capabilities like "Network Contain" to isolate impacted endpoints and to collect evidence • Know your log data retention periods • Forensic Analysts will follow Indicators of Compromise to uncover details • Don't wipe or restore anything until you are told it's okay to do so
Engage your IR Plan and claims process immediately	• Have your Incident Response Team identified and prepared to act • Know who is responsible for activating the incident response plan • Know what conditions would trigger the activation of the Incident Response Plan • Ensure IR Team understands their roles and responsibilities • Be prepared to communicate offline from your normal communication channels
Manage communication and notification obligations	• Know your notification obligations and timelines in advance • Be prepared to notify authorities, clients, third-parties, and others that may experience impacts
Learn and improve	• Recorrect user behavior that led to a breach or compromise • Conduct a post-incident review to improve your security and future responses

NLS CYBERSECURITY

RESOURCES

RLS CYBERSECURITY

RESOURCES

CYBER INCIDENT READINESS CHECKLIST

CYBERSECURITY PLAYBOOK

2026 CYBER STRATEGY PROGRAM

FREE CYBER STRATEGY SESSION

RLS CYBERSECURITY

RISK CONTROL OUTREACH – MAY 2026

Flood & Peterson

THANK YOU FOR JOINING!

GETTING HELP

CYBER STRATEGY PROGRAM & RESOURCES COLLECTION

rlsconsulting.co/2026cyberstrategyprogram

BOOK A CYBER STRATEGY SESSION

rlsconsulting.co/freecyberconsult

CONTACT US

ryan@rlsconsulting.co

RLS CYBERSECURITY