CENTARIS™

Security Awareness Training:

how to protect yourself and your business with a humans first approach

CENTARIS™

www.Centaris.com

What you need to know!

- Insight into some popular cyber threats in today's landscape. Real life examples of how they occur.

- Some of the ways you can prevent similar threats to protect your Customers, Employees and your Business.

Let's Look beyond hardware and technology and into human behavior to see your risk and value.

THE STATE OF CYBERSECURITY TODAY

350% On average an employee at a small business will receive 350% more social engineering attacks than employees of larger enterprises.

61% 61% of Small Businesses reported at least one cyber attack last year.

83% 83% of small businesses haven't purchased cyber liability insurance to protect themselves in a breach

14% Only 14% of small businesses consider their cyber attack and risk mitigation ability as highly effective.

THE STATE OF CYBERSECURITY TODAY

SMALL BUSINESSES ARE TARGETED MORE OFTEN AND ARE AT A HIGHER RISK BECAUSE THEY LACK JUST AS MANY SECURITY RESOURCES AND EXPERTISE AS LARGER ENTERPRISES.

CYBER CRIMINALS HAVE FIGURED OUT THAT IT'S A LOT EASIER TO CATCH SMALLER FISH RATHER THAN GO AFTER THE BIG FISH!

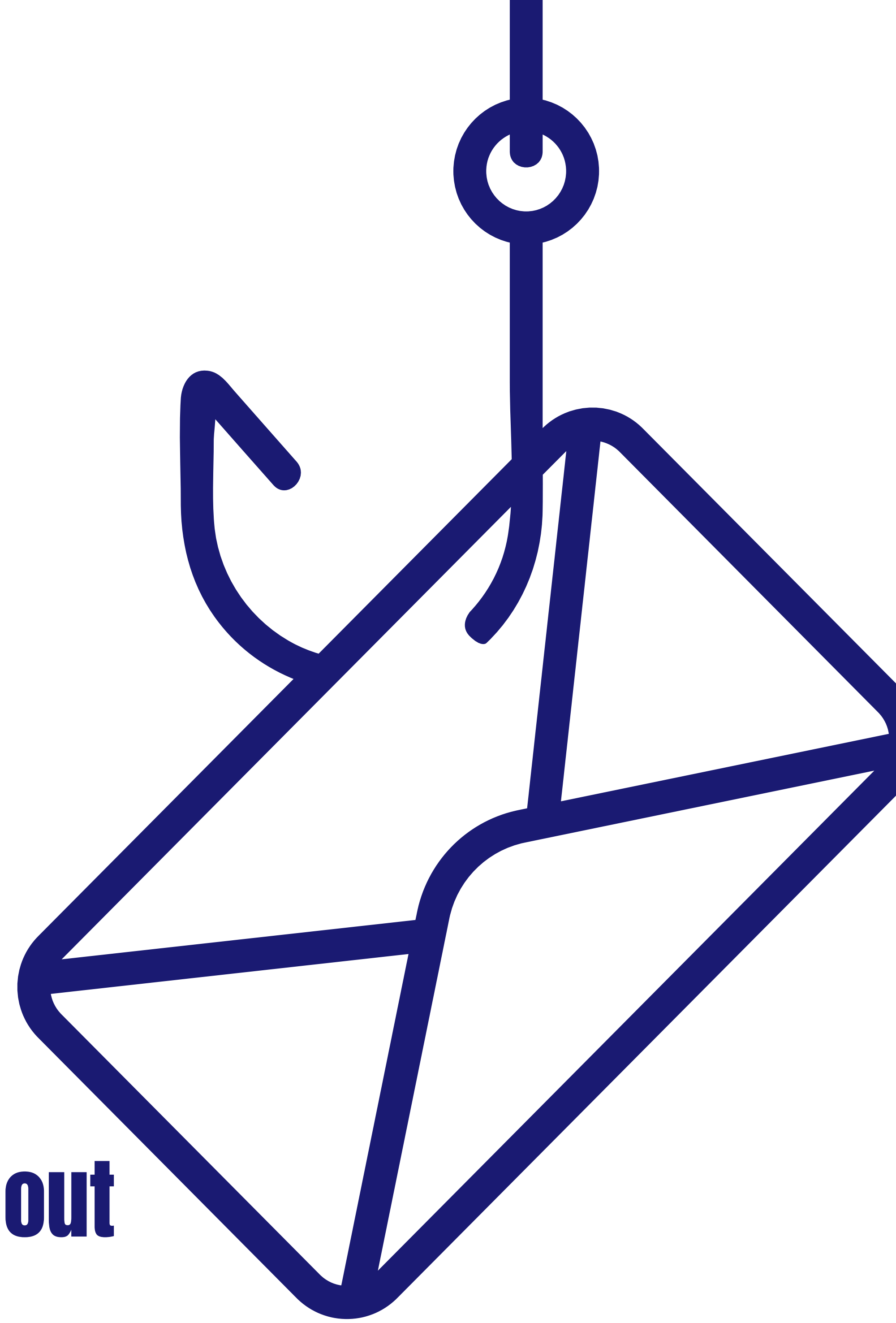
the same threats you've probably been hearing for a long time are getting even more sophisticated.

- Phishing
- Ransomware
- Account take Over

Sophisticated Phishing Attacks

What is a Phishing Attack?

The Evolution of Phishing Attacks



- Mass Phishing-Generic email to thousands or millions of people.

- Spear Phishing-Email targeting a specific individual using information they know about them.

- Business Email Compromise (BEC)-Multi step attack to trick email recipients into believing someone they know and trust is asking them to carry out a specific task.

The Story of BEC: Vectors for attack

Cyber Criminals will impersonate:

A CEO or other executive

HR personnel

A Trusted Vendor

Goals for BEC:

Steal sensitive data

Get access to critical systems

Financial fraud (Most popular)

Successful BEC attack of this type cost $180k+ on Average

Source: 2021 FBI Internet Crime Report

The Story of a BEC

Vendor Email Compromise, between a healthcare company and their medical supplier

Meet the Victims:

Mariah Carey works at a medical supply company (Vendor A)

Tom Cruise is the Office Manager at the medical client (Client B)

Meet the cyber criminal:

What a jerk.

The actual Story...

Mariah Carey (Vendor A) had the credentials of her email account compromised!

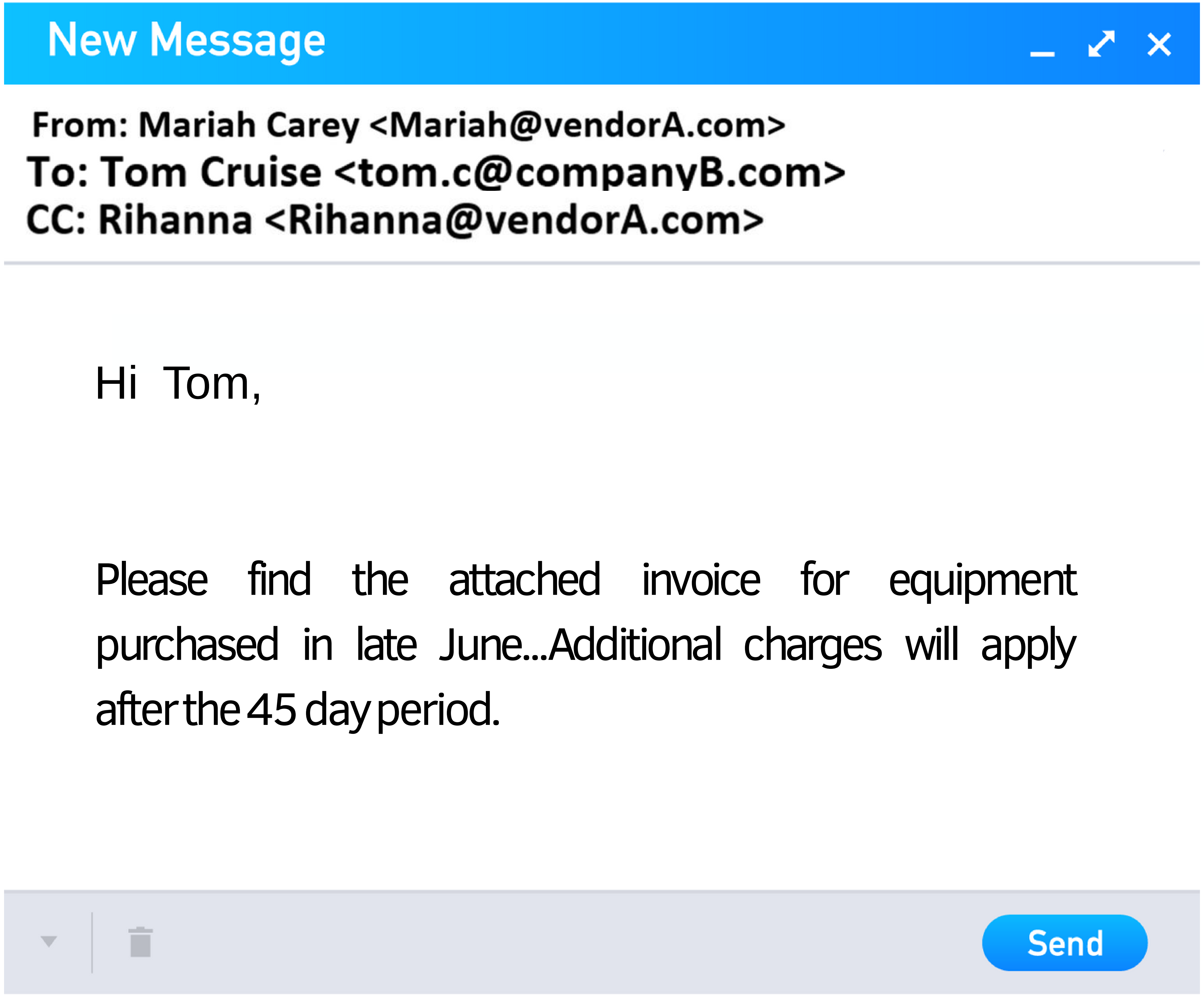
There are many ways that this could have happened: Mass Phishing, Dark Web Breach, Bad password controls; we'll come back to this later.

The cyber criminal uses these compromised credentials to access her account and set up a rule that forwards all of her mail to one of his email accounts

The Cyber Criminal then waits and watches the normal interactions Mariah at Vendor A has with her clients, waiting for the right moment to strike.

The right moment

A legitimate invoice is sent from the Vendor to Client



From: Mariah Carey <Mariah@vendorA.com>
To: Tom Cruise <tom.c@companyB.com>
CC: Rihanna <Rihanna@vendorA.com>

Hi Tom,

Please find the attached invoice for equipment purchased in late June...Additional charges will apply after the 45 day period.

Ready to Strike

The cyber criminal now already has:

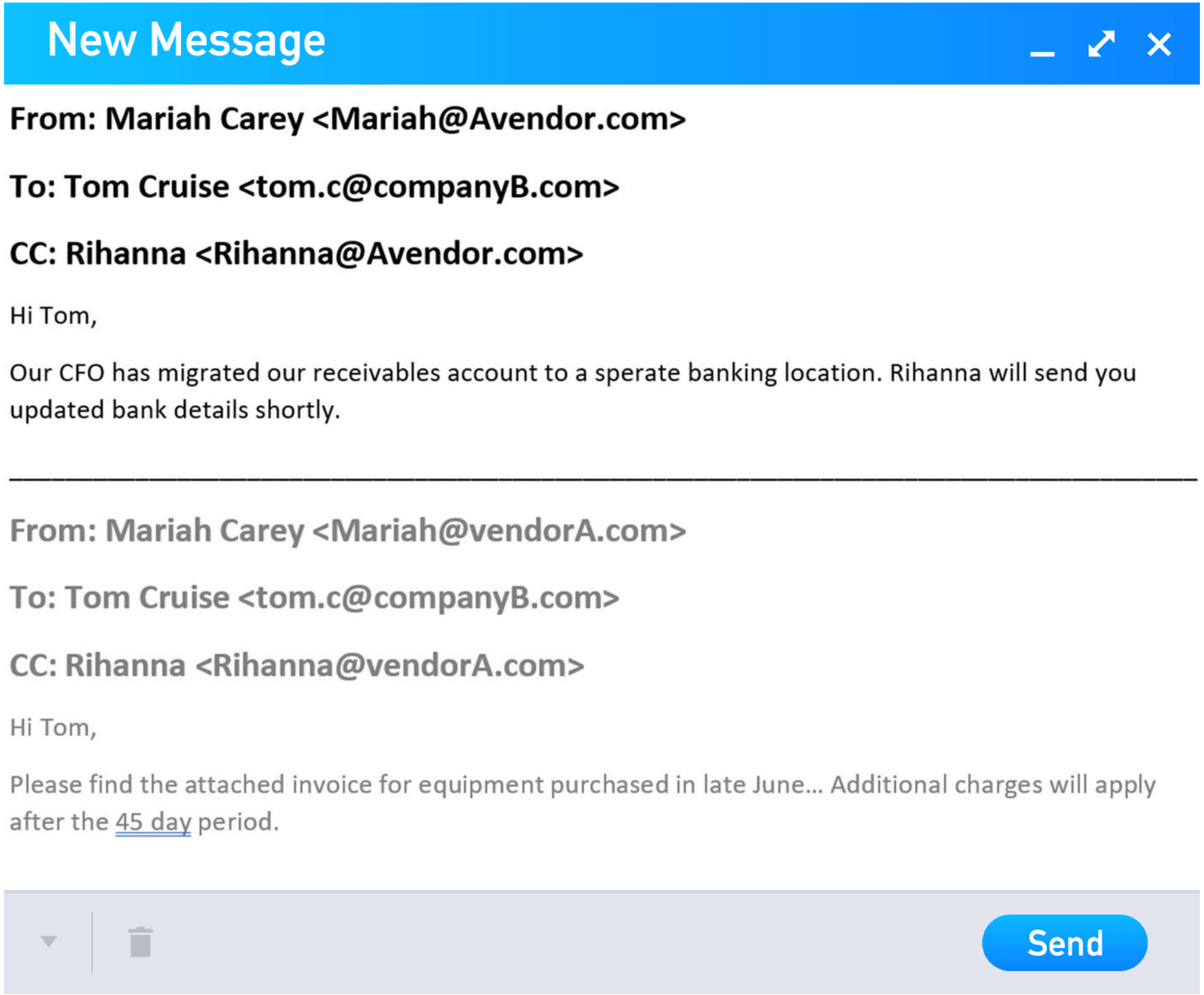
- Purchased a fake email domain
- Created a bank account with fake details

Real Email of Vendor A

Mariah Carey <Mariah@vendorA.com> → **Mariah Carey <Mariah@Avendor.com>**

Real Email of Company B

The fake email domain is cheap to buy and looks very similar, this is just a mirror of the first domain name. In the actual attack that the medical client had the 3 word name of their company as their domain and the attacker dropped 1 word from it.



From: Mariah Carey <Mariah@Avendor.com>

To: Tom Cruise <tom.c@companyB.com>

CC: Rihanna <Rihanna@Avendor.com>

Hi Tom,

Our CFO has migrated our receivables account to a sperate banking location. Rihanna will send you updated bank details shortly.

From: Mariah Carey <Mariah@vendorA.com>

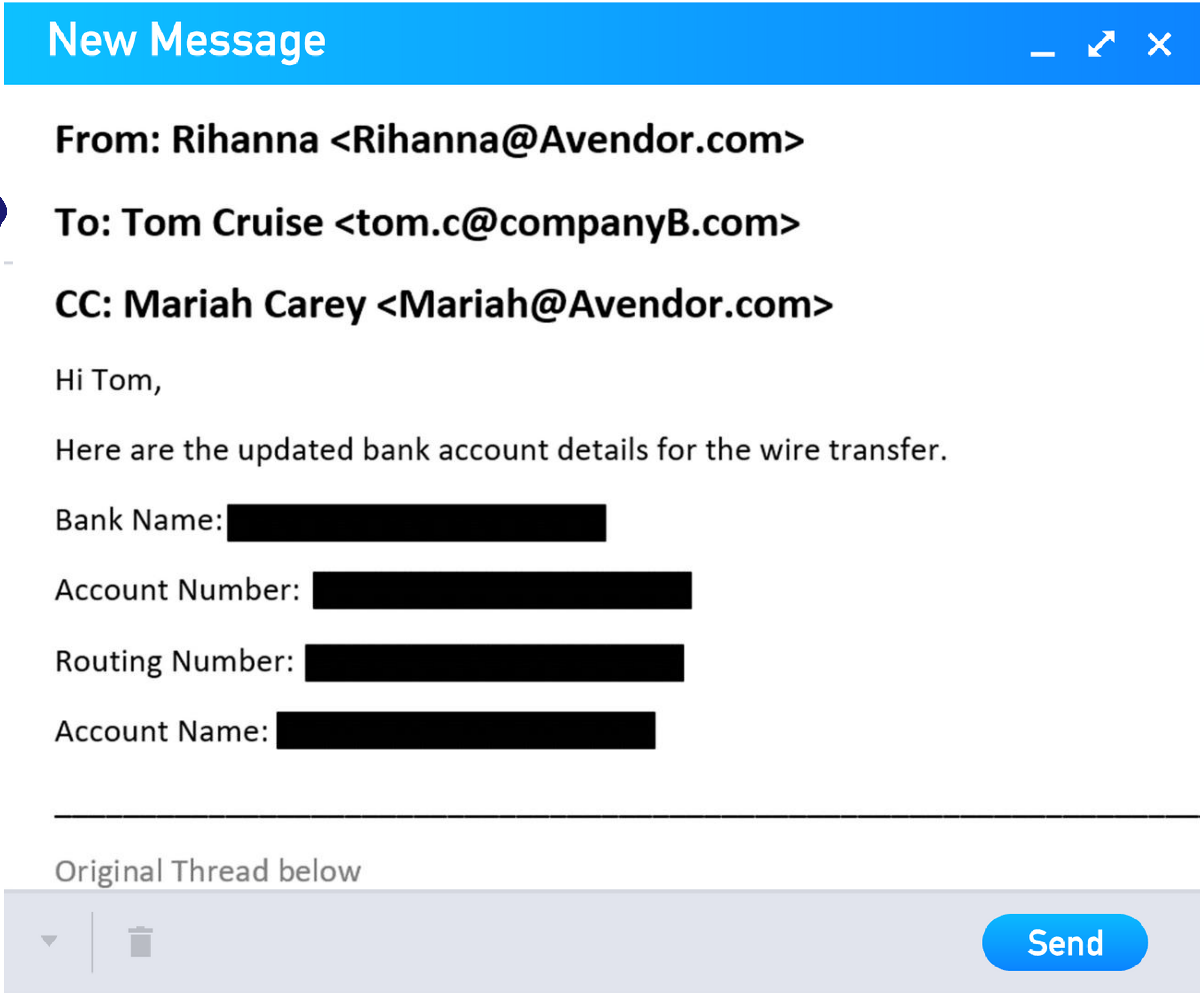
To: Tom Cruise <tom.c@companyB.com>

CC: Rihanna <Rihanna@vendorA.com>

Hi Tom,

Please find the attached invoice for equipment purchased in late June... Additional charges will apply after the 45 day period.

Added credibility by having another person that was in the thread previously send the information while including the entire original thread



From: Rihanna <Rihanna@Avendor.com>

To: Tom Cruise <tom.c@companyB.com>

CC: Mariah Carey <Mariah@Avendor.com>

Hi Tom,

Here are the updated bank account details for the wire transfer.

Bank Name: [redacted]

Account Number: [redacted]

Routing Number: [redacted]

Account Name: [redacted]

Original Thread below

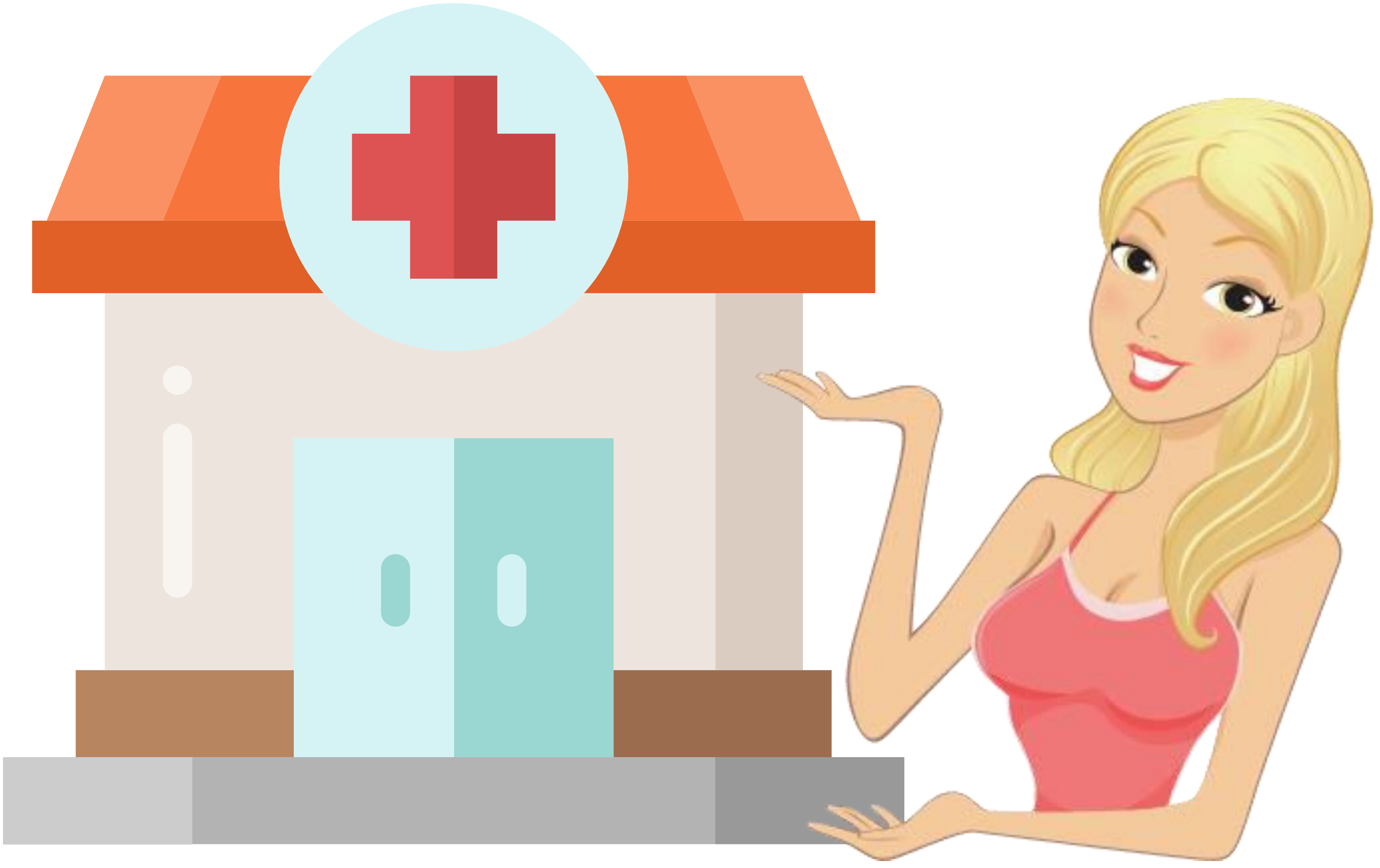
WHO IN YOUR COMPANY WOULD HAVE SPOTTED THIS?

The Damage

Company B

-Tom at Company B sent $50K the first time

-And $100k the second time one week later



Vendor A

-Loss off Company B as a client

-Further reputation damage with their other clients

-Possible future litigation with Company B

How this could have been avoided?

BOTH VENDOR A AND CUSTOMER B HAVE NEGATIVE IMPACT TO THEIR BUSINESS

Vendor A had their email account compromised

Implement good password hygiene to reduce password reuse

Adopt a Multifactor Authentication on their email accounts

Participate in on-going training on how to avoid phishing scams

Company B was as a sitting target without even knowing it

They need to require a strong P&P for handling wire transfers

Participate in Phishing detection simulation to potentially be able to spot an attack like this

Continuously Educate their employees on how to spot phishing emails

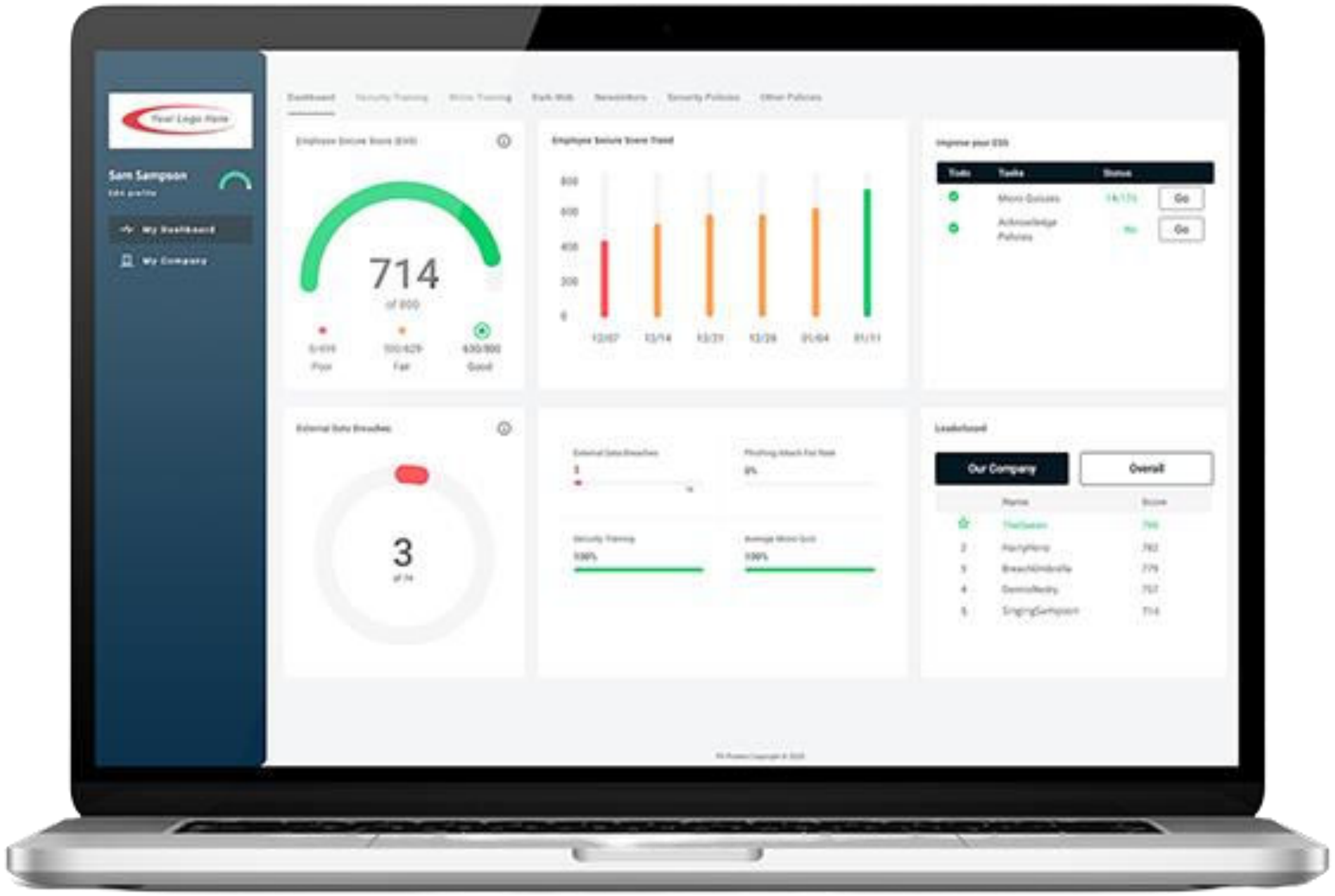
WHAT WE ARE GOING TO DO ABOUT IT. TOGETHER

Scams are becoming more sophisticated and you cannot rely on an in the box solution to protect yourself and your company.

You need a multi layer approach and a culture of cybersecurity in your company!

CCare Security Awareness PII-Protect Management and Monitoring

End-User Education, Evolved



- → Dark Web Monitoring
- → Weekly Micro-Training Video & Quiz
- → Unlimited Simulated Phishing Campaigns
- → Monthly Security Newsletter
- → Security Risk Assessment
- → Written Security Policies
- → Catch Phish
- → Employee Vulnerability Assessment
- → Cybersecurity Newsfeed

Employee Vulnerability Assessment (EVA): The heart of the PII-Protect

Combines proven security metrics with quantitative analysis and friendly competition to offer unparalleled insight into an organization's first layer of defense - *their employees*.

Employee Secure Score (ESS)

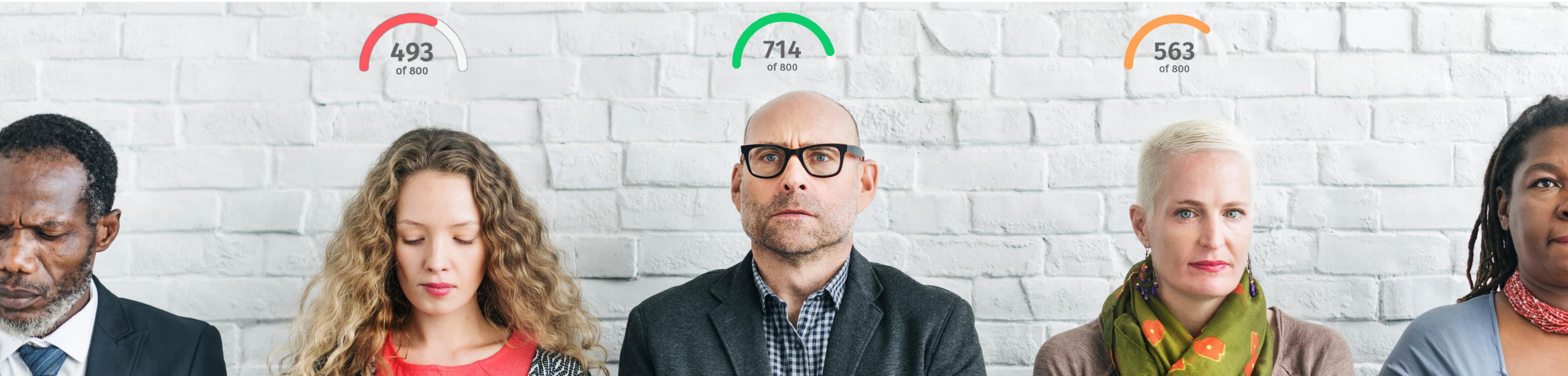
Which employee is the weakest link?

The ESS uses a sophisticated algorithm of metrics to transform end-user education into an analytical engine. By assigning an ESS to each user, employees can see where they fall in their peer group and in what areas they can improve.

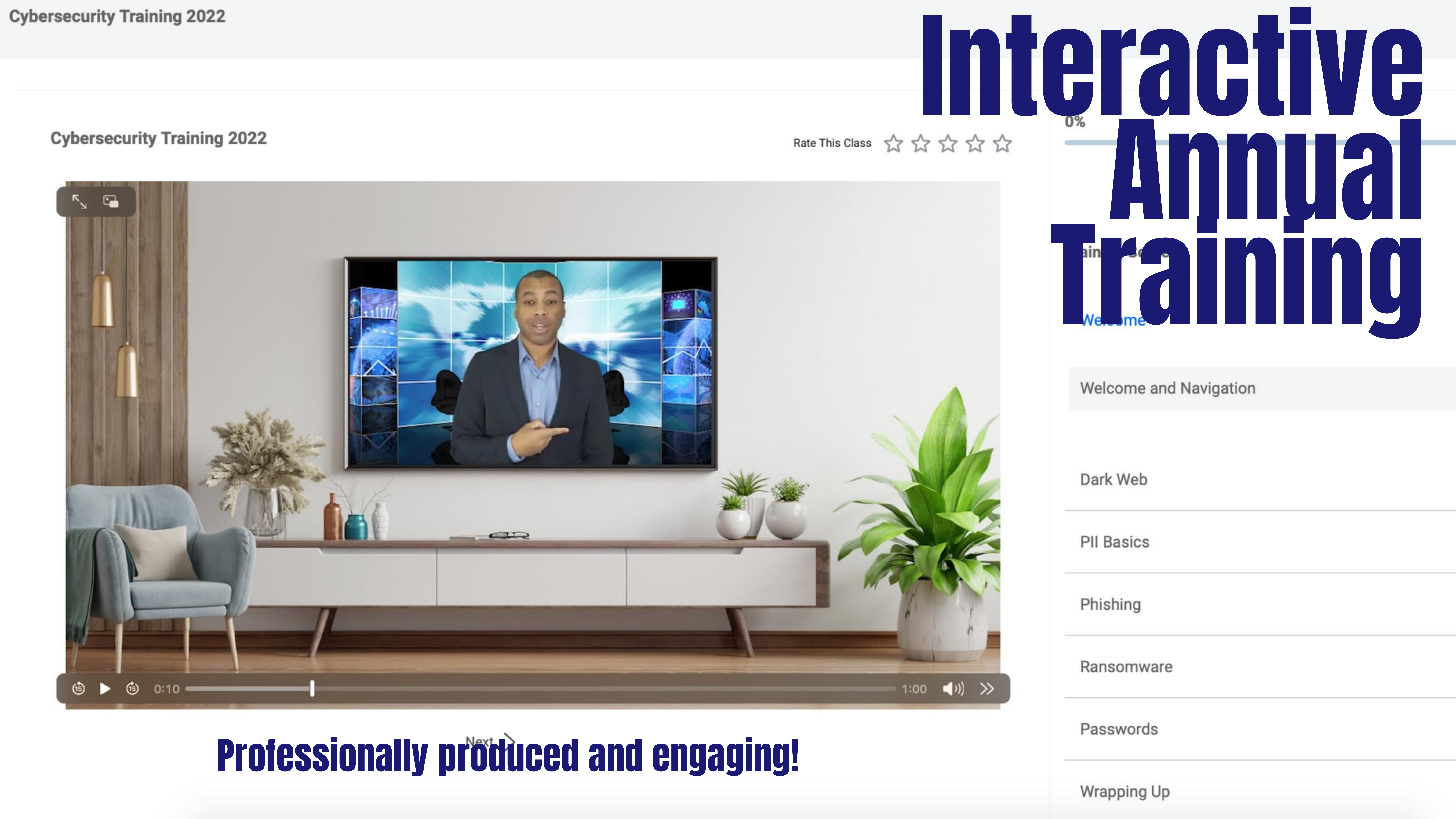
Company Overall ESS

How will you reduce their risk level?

By averaging all end-users' ESS', each organization is assigned a Company Overall ESS. Leveraging this score gives management insight into their overall security hygiene and highlights the need for technical safeguards.



Interactive Annual Training



Cybersecurity Training 2022

Cybersecurity Training 2022

Rate This Class ☆ ☆ ☆ ☆ ☆

0%

Welcome

Welcome and Navigation

Dark Web

PII Basics

Phishing

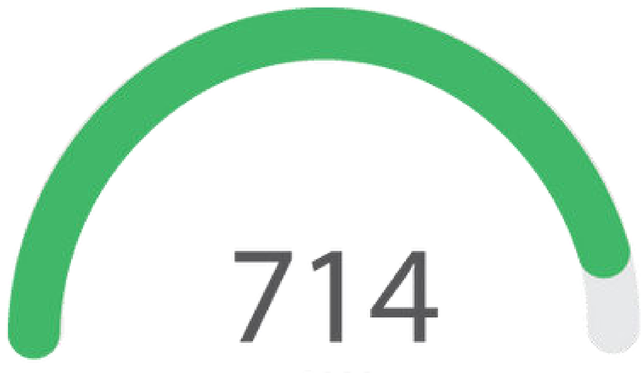
Ransomware

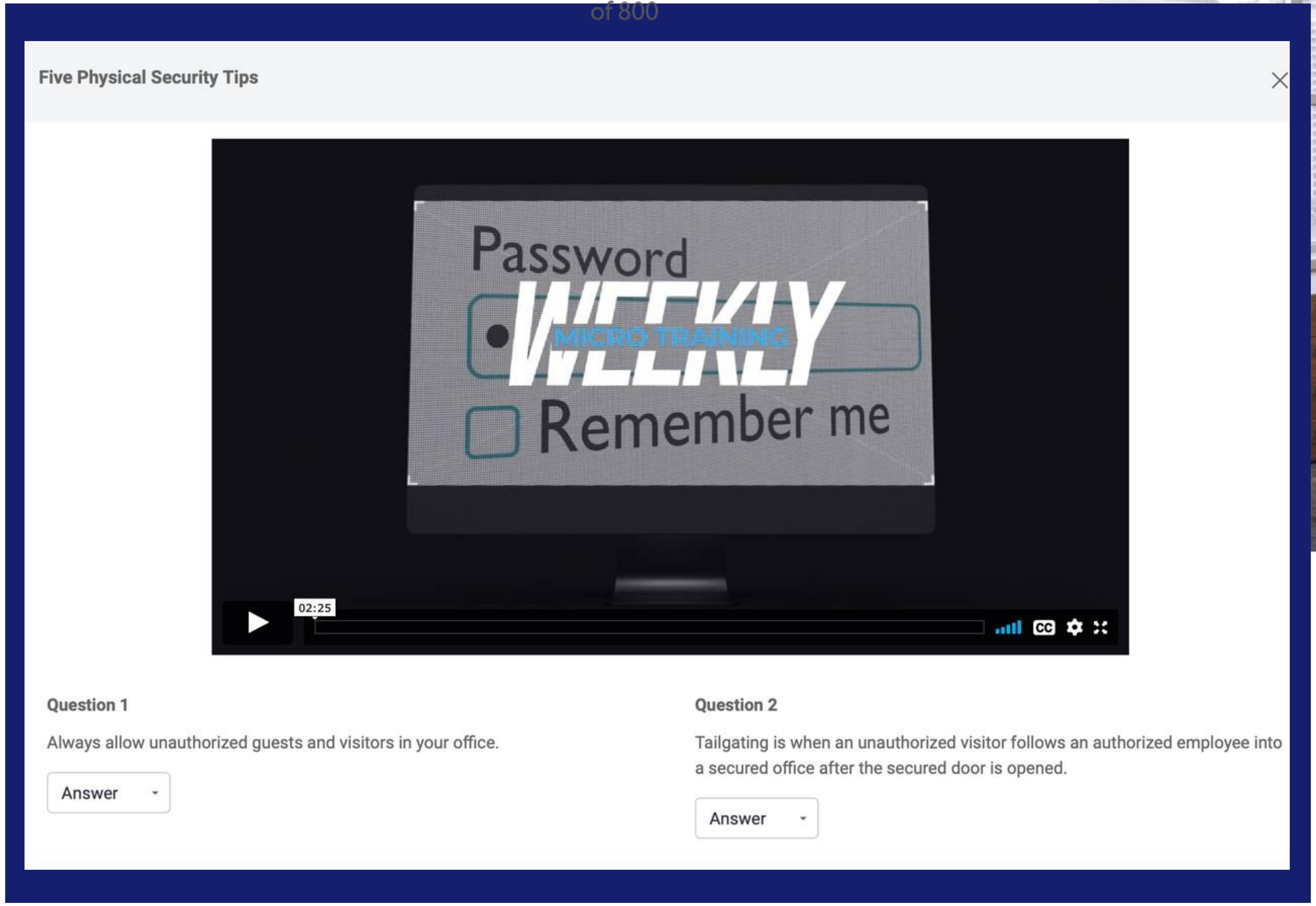
Passwords

Wrapping Up

Professionally produced and engaging!

Weekly Micro-Trainings





Five Physical Security Tips

Question 1

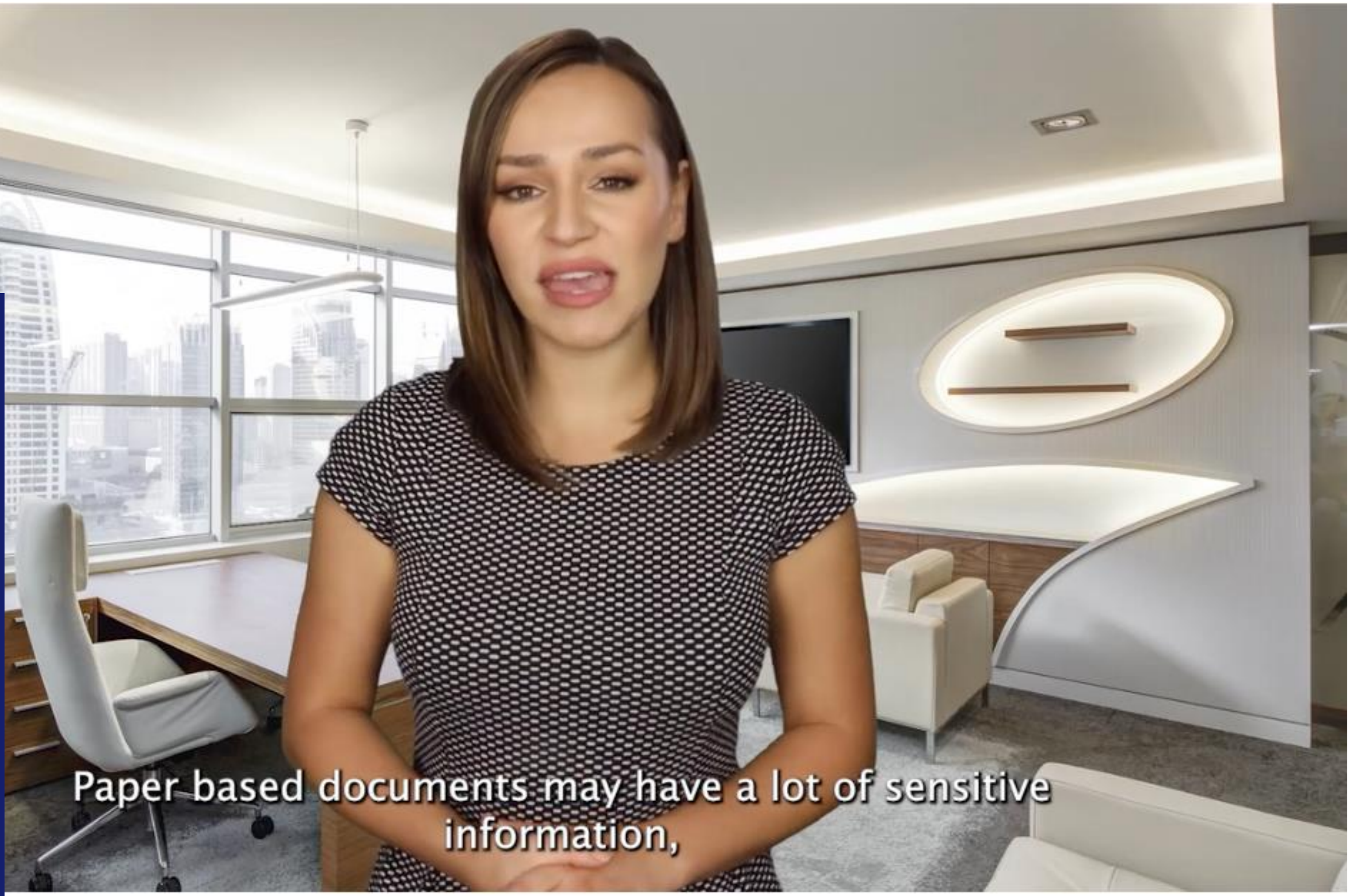
Always allow unauthorized guests and visitors in your office.

Answer

Question 2

Tailgating is when an unauthorized visitor follows an authorized employee into a secured office after the secured door is opened.

Answer



Paper based documents may have a lot of sensitive information,

Perfect!

You answered 4 out of 4 questions correct

Monthly Newsletters

SCAM CULTURE

Did scamming just get cooler?

THIS MONTH'S TOPICS:

Scamming the Scammer

Don't pick up the phone...

#NonFiction

"Scam Culture" is making its way into a hot, new sub-genre!

But, in order to keep these types of stories engaging, mainstream media often shows the glamorous side of

CYBER SHADOWS

The dark side of the cyber world that follows you around

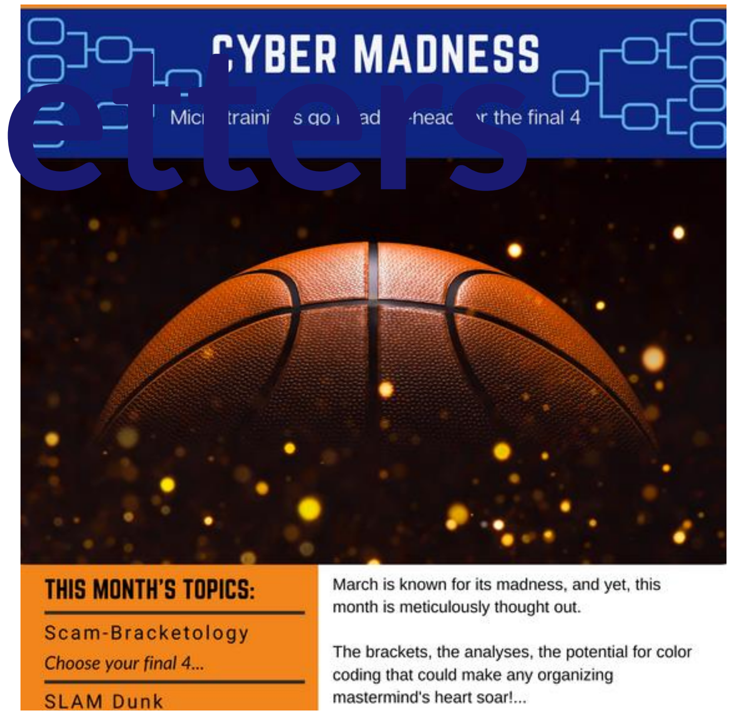
THIS MONTH'S TOPICS:

The Profile

The shadows that follow you on Social...

There's no doubt that there is a dark side of the internet, but have you ever felt like it was following you around?

Scammers can lurk right behind every online



CYBER MADNESS

Microtrainings go head-to-head for the final 4

THIS MONTH'S TOPICS:

Scam-Bracketology

Choose your final 4...

SLAM Dunk

March is known for its madness, and yet, this month is meticulously thought out.

The brackets, the analyses, the potential for color coding that could make any organizing mastermind's heart soar!...

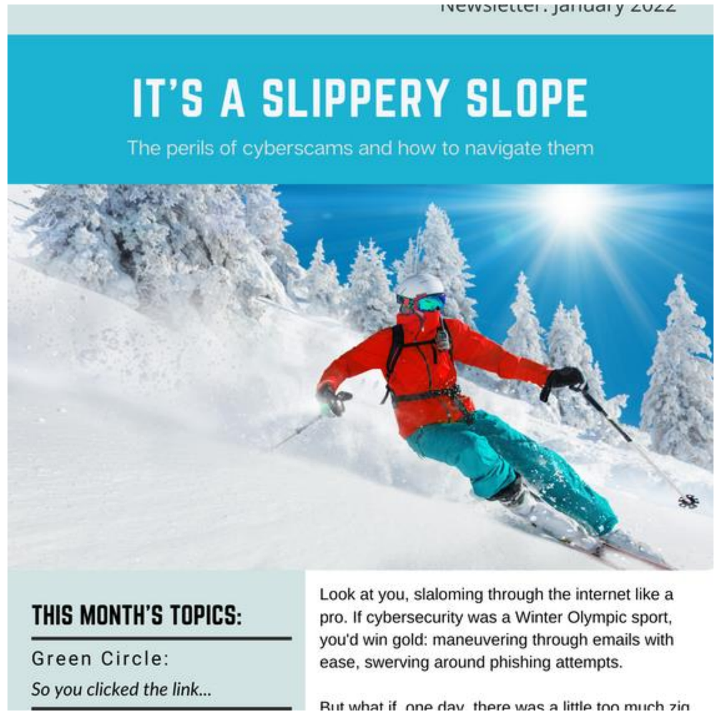
Newsletter: August 2021

CYBERSECURITY FOR OUR OLDER GENERATION

A review of the latest security threats and how you can avoid them

THIS MONTH'S TOPICS:

Our elders have been shaping our path to maturity with their life lessons, words of wisdom and other guidance meant to educate us on right from wrong. It's time for us to return the favor for them!



Newsletter: January 2022

IT'S A SLIPPERY SLOPE

The perils of cyberscams and how to navigate them

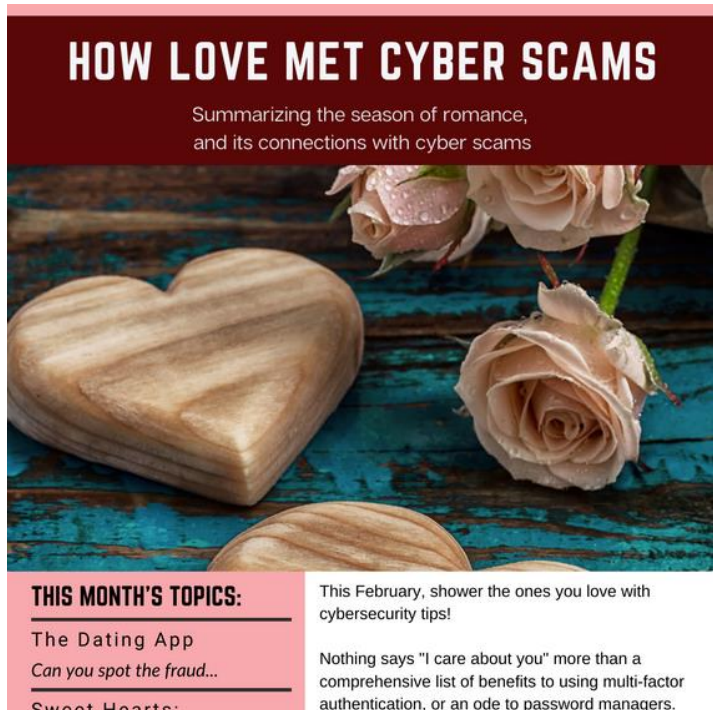
THIS MONTH'S TOPICS:

Green Circle:

So you clicked the link...

Look at you, slaloming through the internet like a pro. If cybersecurity was a Winter Olympic sport, you'd win gold: maneuvering through emails with ease, swerving around phishing attempts.

But what if, one day, there was a little too much zig



HOW LOVE MET CYBER SCAMS

Summarizing the season of romance, and its connections with cyber scams

THIS MONTH'S TOPICS:

The Dating App

Can you spot the fraud...

Sweet Hearts:

This February, shower the ones you love with cybersecurity tips!

Nothing says "I care about you" more than a comprehensive list of benefits to using multi-factor authentication, or an ode to password managers.

WHEN IT RAINS, IT POURS

Examining the splash back of a breach on a company

THIS MONTH'S TOPICS:

Light Drizzle

Small businesses and breaches...

Monsoon Season

April likes to rain a lot, and scammers like to scam a lot.

So what happens when you're unaware of today's weather, and you venture out, sans umbrella? The same thing that's likely to happen when you're un-cyberaware, surfing the internet: you get drenched, and it's not pretty.

CYBERSECURITY FOR OUR YOUNGER GENERATION

A review of the latest security threats and how you can avoid them

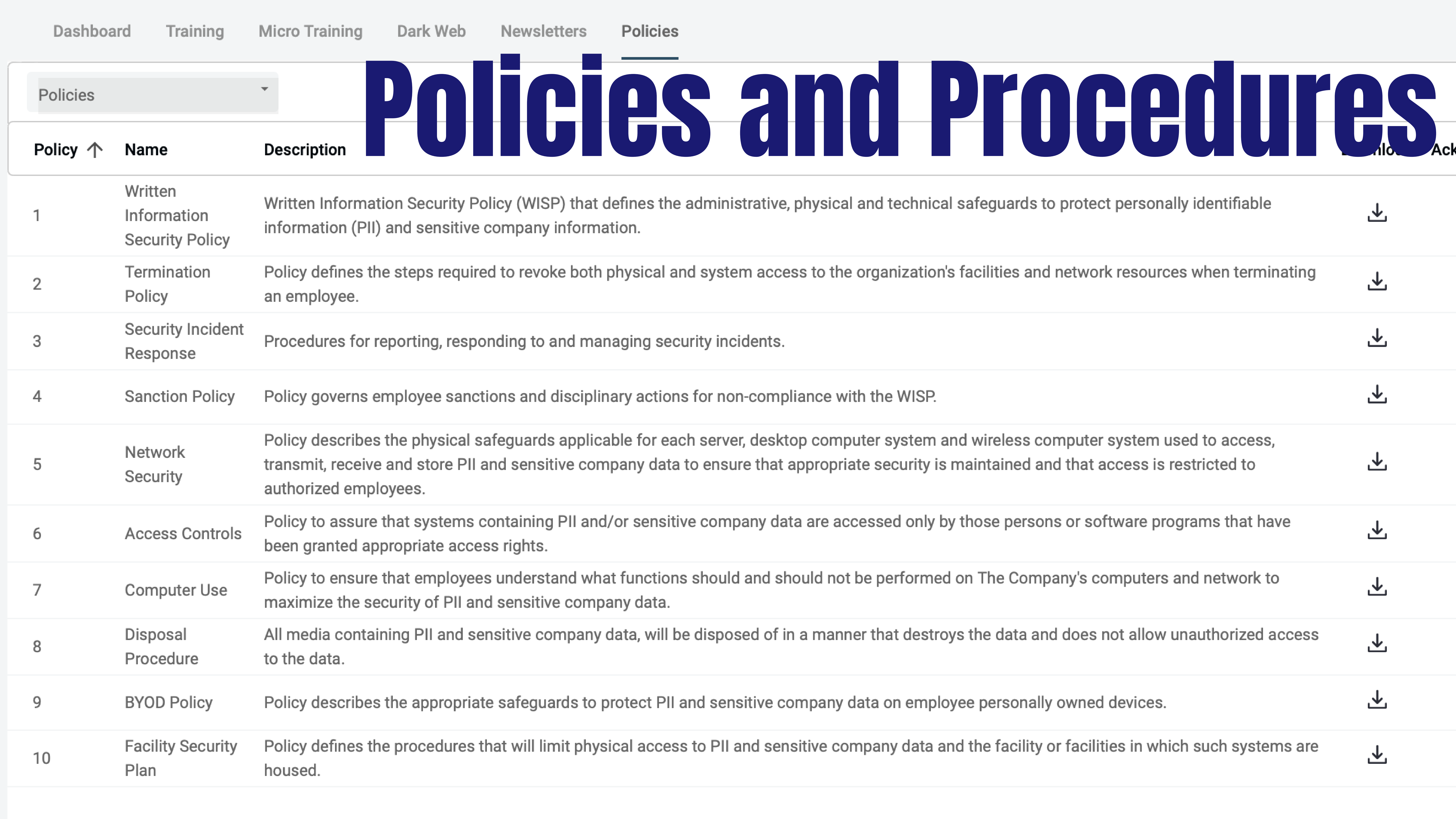
THIS MONTH'S TOPICS:

Navigating the Cybersecurity Path of

Cybercrime and the digital risks we face are showing no signs of slowing down. Although tools, resources, and past experiences have helped *us* prepare for some of these cybersecurity threats, the same opportunities may not be readily available to our children or the younger generation.

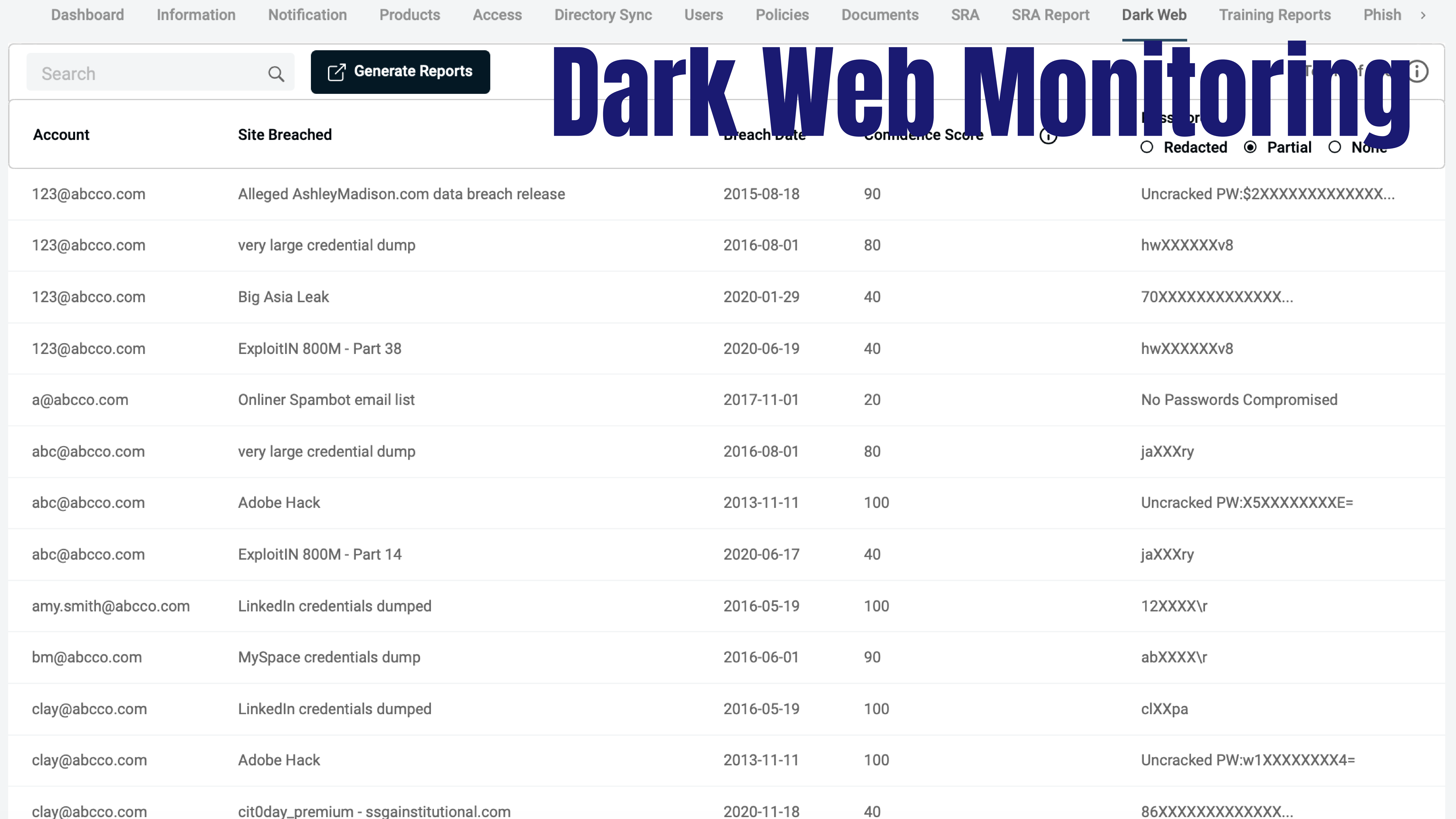
CENTARIS™

Policies and Procedures



Policy ↑	Name	Description	nlo	Ack
1	Written Information Security Policy	Written Information Security Policy (WISP) that defines the administrative, physical and technical safeguards to protect personally identifiable information (PII) and sensitive company information.	⤓	
2	Termination Policy	Policy defines the steps required to revoke both physical and system access to the organization's facilities and network resources when terminating an employee.	⤓	
3	Security Incident Response	Procedures for reporting, responding to and managing security incidents.	⤓	
4	Sanction Policy	Policy governs employee sanctions and disciplinary actions for non-compliance with the WISP.	⤓	
5	Network Security	Policy describes the physical safeguards applicable for each server, desktop computer system and wireless computer system used to access, transmit, receive and store PII and sensitive company data to ensure that appropriate security is maintained and that access is restricted to authorized employees.	⤓	
6	Access Controls	Policy to assure that systems containing PII and/or sensitive company data are accessed only by those persons or software programs that have been granted appropriate access rights.	⤓	
7	Computer Use	Policy to ensure that employees understand what functions should and should not be performed on The Company's computers and network to maximize the security of PII and sensitive company data.	⤓	
8	Disposal Procedure	All media containing PII and sensitive company data, will be disposed of in a manner that destroys the data and does not allow unauthorized access to the data.	⤓	
9	BYOD Policy	Policy describes the appropriate safeguards to protect PII and sensitive company data on employee personally owned devices.	⤓	
10	Facility Security Plan	Policy defines the procedures that will limit physical access to PII and sensitive company data and the facility or facilities in which such systems are housed.	⤓	

Dark Web Monitoring



Account	Site Breached	Breach Date	Confidence Score	Password ○ Redacted ● Partial ○ None
123@abcco.com	Alleged AshleyMadison.com data breach release	2015-08-18	90	Uncracked PW:$2XXXXXXXXXXXX...
123@abcco.com	very large credential dump	2016-08-01	80	hwXXXXXXv8
123@abcco.com	Big Asia Leak	2020-01-29	40	70XXXXXXXXXXXXX...
123@abcco.com	ExploitIN 800M - Part 38	2020-06-19	40	hwXXXXXXv8
a@abcco.com	Onliner Spambot email list	2017-11-01	20	No Passwords Compromised
abc@abcco.com	very large credential dump	2016-08-01	80	jaXXXry
abc@abcco.com	Adobe Hack	2013-11-11	100	Uncracked PW:X5XXXXXXXXE=
abc@abcco.com	ExploitIN 800M - Part 14	2020-06-17	40	jaXXXry
amy.smith@abcco.com	LinkedIn credentials dumped	2016-05-19	100	12XXXX\r
bm@abcco.com	MySpace credentials dump	2016-06-01	90	abXXXX\r
clay@abcco.com	LinkedIn credentials dumped	2016-05-19	100	clXXpa
clay@abcco.com	Adobe Hack	2013-11-11	100	Uncracked PW:w1XXXXXXXX4=
clay@abcco.com	cit0day_premium - ssgainstitutional.com	2020-11-18	40	86XXXXXXXXXXXXX...

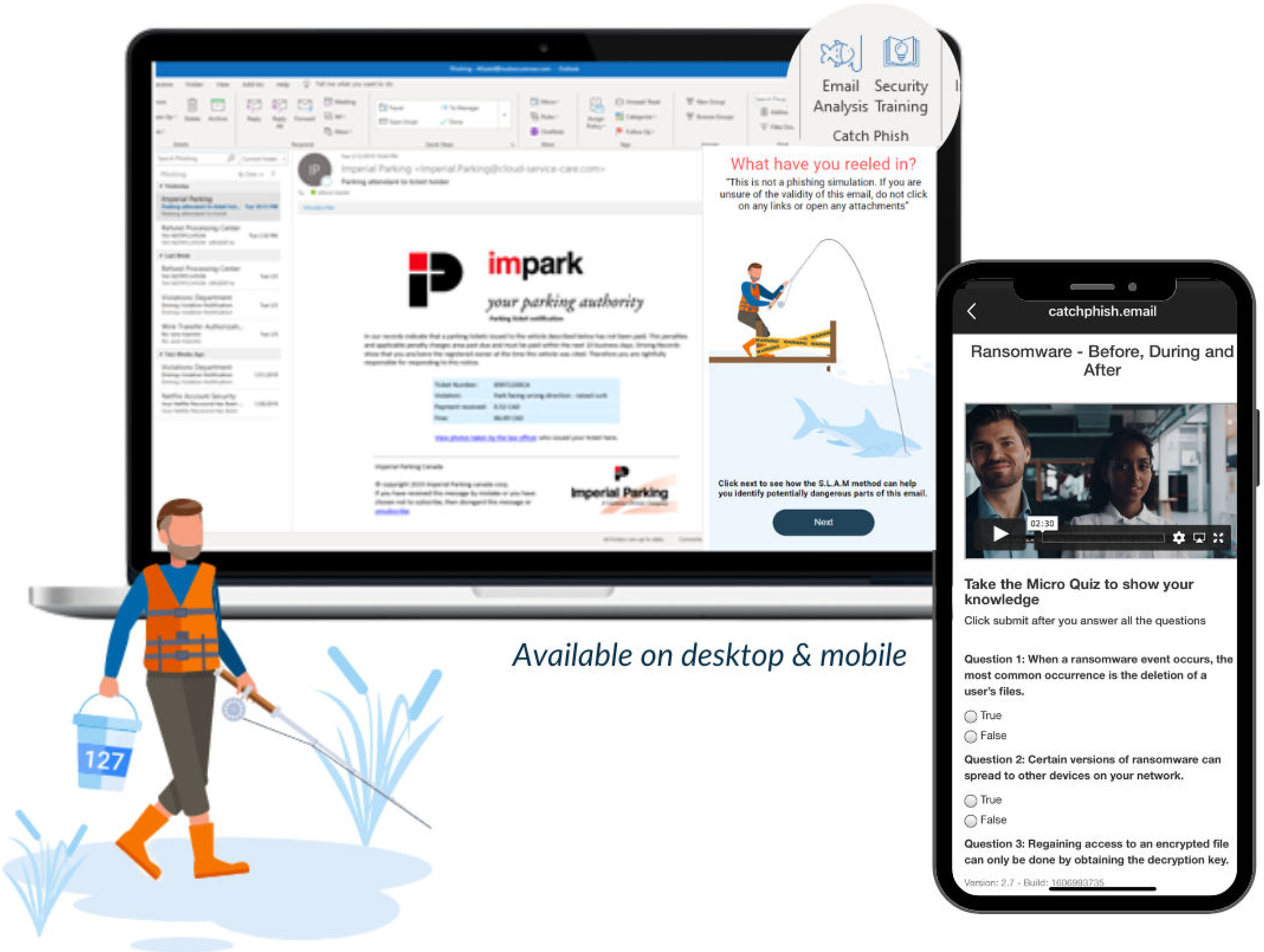
Catch Phish Outlook Plug-In

CENTARIS™

Combat cybercrime where employees are most vulnerable – their inbox.

Catch Phish integrates with Office 365 subscriptions as an add-in.

When an email is analyzed by the tool, Catch Phish will highlight elements of the SLAM Method for further analysis.



What have you reeled in?

"This is not a phishing simulation. If you are unsure of the validity of this email, do not click on any links or open any attachments"

Click next to see how the S.L.A.M method can help you identify potentially dangerous parts of this email.

Next

Ransomware - Before, During and After

Take the Micro Quiz to show your knowledge

Click submit after you answer all the questions

Question 1: When a ransomware event occurs, the most common occurrence is the deletion of a user's files.

○ True
○ False

Question 2: Certain versions of ransomware can spread to other devices on your network.

○ True
○ False

Question 3: Regaining access to an encrypted file can only be done by obtaining the decryption key.

Version: 2.7 - Build: 1606983735

Available on desktop & mobile

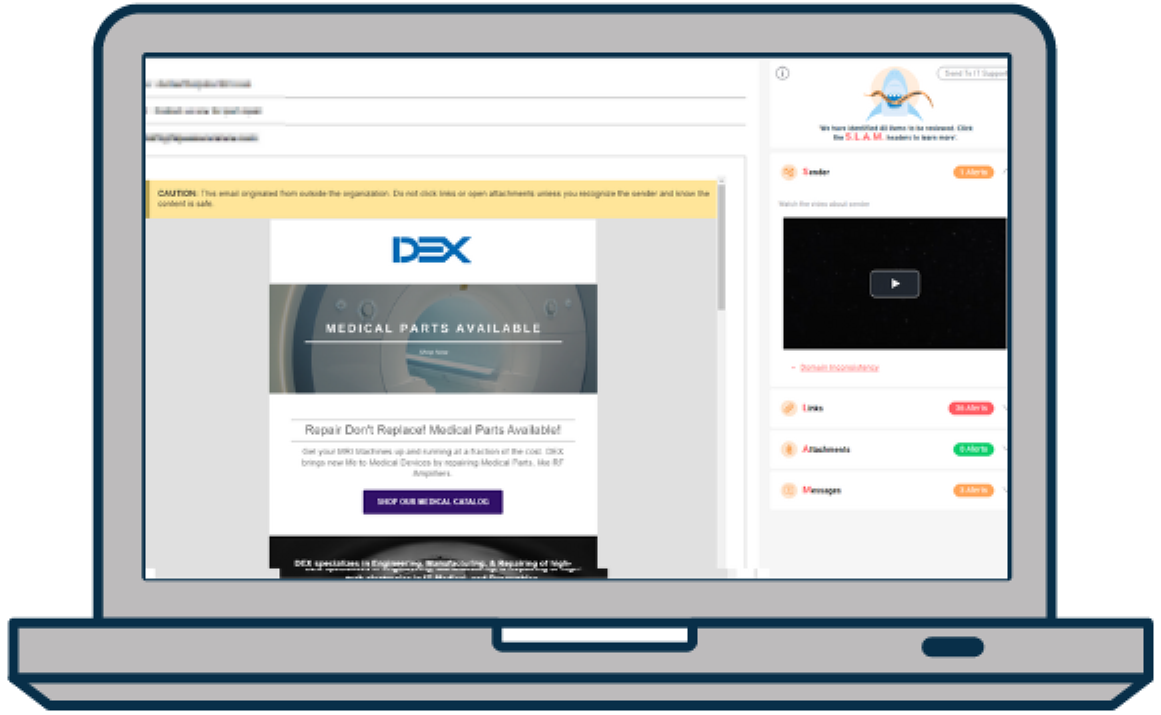
Catch Phish Outlook Plug-In

Users can click the button in their toolbar to leverage machine learning and AI to confidently verify the legitimacy of any email that hits their inbox.

Email Analysis:

Click.

Catch Phish's Email Analysis feature gives you the tools to instantly analyze emails for malicious links, language, attachments, and other hidden elements. **Within seconds your client will know if that link is safe to click or if that request from the CEO could be a cybercriminal impersonating their account.**



CAUTION: This email originated from outside the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.

DEX

MEDICAL PARTS AVAILABLE

Repair Don't Replace! Medical Parts Available!

Get your MRI Machines up and running at a fraction of the cost. DEX brings new life to Medical Devices by repairing Medical Parts, like RF Amplifiers.

SHOP OUR MEDICAL CATALOG

We have identified all items to be reviewed. Click the S.L.A.M. headers to learn more.

No more guessing, no more waiting for a tech to confirm suspicions, just instant insight that fills in the gaps and makes decision making, simple.

Once the scan is complete, a total number of alerts through the four categories will be identified and easily indicated. By hovering over the identified components of the analysis, users can learn more about why the area was identified and learn more about any red flags.

CENTARIS™

The new and improved tool now scans emails through the lens of the SLAM method. Highlighting 4 important elements for the user to further consider.

SLAM

The Scam

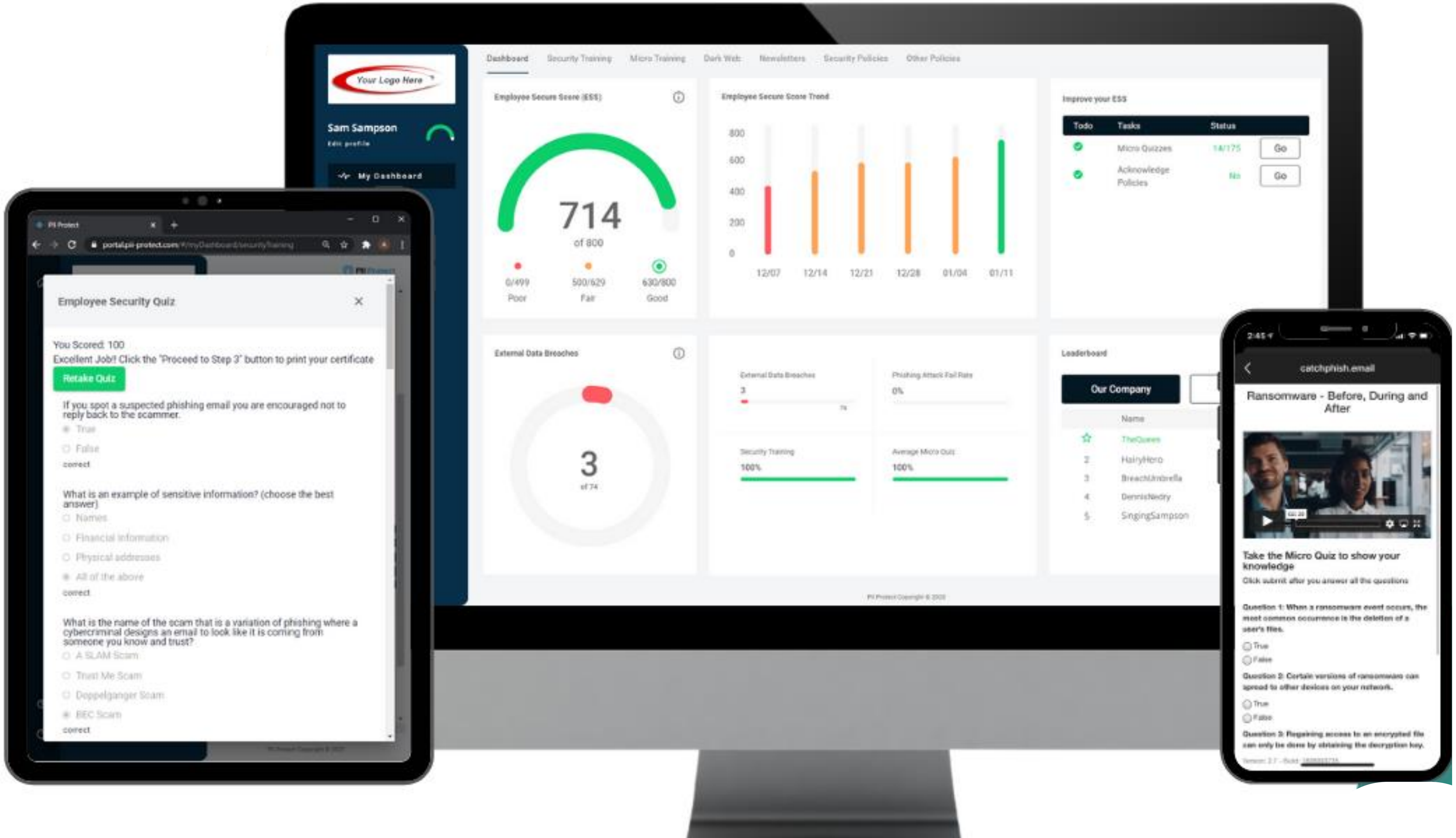
Sender

Links

Attachments

Message

CENTARIS™



Todo	Tasks	Status	
✓	Micro Quizzes	14/175	Go
✓	Acknowledge Policies	No	Go

	Name
☆	TheQueen
2	HairyHero
3	BreachUmbrella
4	DennisNedry
5	SingingSampson

PII Protect

portal.pii-protect.com/#/myDashboard/securityTraining

Employee Security Quiz ✕

You Scored: 100

Excellent Job!! Click the "Proceed to Step 3" button to print your certificate

Retake Quiz

If you spot a suspected phishing email you are encouraged not to reply back to the scammer.

● True

○ False

correct

What is an example of sensitive information? (choose the best answer)

○ Names

○ Financial information

○ Physical addresses

● All of the above

correct

What is the name of the scam that is a variation of phishing where a cybercriminal designs an email to look like it is coming from someone you know and trust?

○ A SLAM Scam

○ Trust Me Scam

○ Doppelganger Scam

● BEC Scam

correct

Ransomware - Before, During and After

Take the Micro Quiz to show your knowledge

Click submit after you answer all the questions

Question 1: When a ransomware event occurs, the most common occurrence is the deletion of a user's files.

○ True

○ False

Question 2: Certain versions of ransomware can spread to other devices on your network.

○ True

○ False

Question 3: Regaining access to an encrypted file can only be done by obtaining the decryption key.

RANSOMWARE IS ALIVE AND WELL.

CENTARIS™

RANSOMWARE ON AVERAGE HITS A SMALL BUSINESS
400,000 TIMES PER DAY

CENTARIS™

Thank you for joining us today!

Congratulations on taking an important step toward stronger cybersecurity.