



Security Awareness Training – Industry Pain Points

- 90% of breaches involve humans. AI & machines make attacks easier and faster for threat actors
- Sustainable defense requires creating a culture of Cyber Resilience throughout your staff
- Cyber Security training needs to be kept up to date for the most relevant threats
- Not just a compliance issue, Cyber Security Awareness is increasingly an Organizational failure point
- Executives across the C-Suite (not just IT) are accountable to Boards & Governments with enforceable standards for cybersecurity

Effective, up-to-date Education is your first line of Defence

Reduce financial risks and build long-term resilience



Incumbent Providers are Missing the Mark

- Training is not led by professionals working in the field every day -> *We work with experts with the highest credentials, including certified ethical hackers, to provide constantly evolving content to protect against today's threats*
- Security Awareness Training is not customizable to Company situations and systems -> *We will customize the learning experience for the organization and integrate with existing training systems.*
- Affordability is becoming stretched along side other physical & technical Cyber investments and incumbent bundling pressure -> *We will work with clients on a package that makes great security awareness training irresistible*
- Training today is commonly long, dull and indigestible causing information overload and not good for providing ongoing learning "bites" -> *We provide short, focused multimedia sessions with opportunities to apply learnings to hands-on exercises and ensure transfer of learning suitable for campaigns*

KnowBe4
Human error. Conquered.

proofpoint.

SANS

INFOSEC

mimecast™

KNOWLEDGE
ACCELERATORS

+
PULSAR
SECURITY



Security Awareness Training – Industry Pain Points

- “98% of Breaches Involve the Human Factor” – Kris Lovejoy, Kyndryl⁽¹⁾
- Awareness of Threats Must be Up-to-Date
- Cyber Resilience Needs to be Emphasized
- Cyber Security Awareness can be an Organizational Failure Point
- Executives Across the C-Suite (not just IT) Will be Responsible

Cyber Security Education is the First Line of Defense

Effective Education Reduces Financial Risks and Protects the Organization

(1) Kris Lovejoy, Head of Kyndryl Security & Resilience Global Practice, Cybercrime Radio Podcast; June 12, 2024



Incumbent Providers are Missing the Mark

- Training is not informed by professionals working in the field every day
- Security Awareness Training is not easy to integrate to your systems
- With other technology investments & incumbent bundling pressure, affordability is stretched (particularly for SMB)
- Training today is commonly long, dull and indigestible causing information overload





Cyber Education Platform

Online Cybersecurity Education from the industry's top experts, backed by the modern science of microlearning, and delivered on a fully customizable platform.

Updated @ Speed of Threats

- Top Tier, Practicing Expert Contributors
- Defence Strategies taught by Ethical Hackers
- Weekly and On-demand Threat Notifications
- Dynamic updates to content (Yours and Ours) and Phishing Simulator

Customize to Your Policies

- Microlearning Eases Changes
- I Do, We Do, You Do Authoring
- AI Meta Data Automation
- Branding to Match Internal Systems

Integrated with existing systems

- LMS, Chatbot, Service Management, SCORM, xAPI, ITSM, Azure AD
- Phishing Simulator Game Built-In
- Automated AI-LLM preparation
- MSGraph-Active Directory Automated Persona Grouping

Campaigns that Change Behavior

- Notification Reporting, Remediation & Upskilling Integrated with Phishing Simulator
- Content Delivery by Persona
- Coaching from Experts
- 'Set and Forget' Delivery & Reminders



Content for Knowledge Workers, including those CMMC Certified

Topic	Vid Count	Duration	Courses	Duration
Passwords & Authentication	10	00:24:35	4	01:30:00
Phishing	9	00:25:01	3	00:58:00
Remote Work	4	00:14:56	1	00:21:00
USB/Removable Media	8	00:31:28	4	01:31:00
Security Awareness	4	00:08:42	2	00:27:00
Email	3	00:06:58	0	00:00:00
Network Security	5	00:14:27	2	00:49:00
Ransomware	7	00:22:47	3	01:03:00
Malware	4	00:15:41	1	00:23:00
CUI	9	00:26:08	1	00:33:00
Insider Threat	7	00:18:58	2	00:44:00
AI Security	2	00:11:01	0	00:00:00
GDPR	7	0.02316	1	0.02316
Social Media	6	00:17:49	2	00:37:00
Total	85	04:31:52	26	09:29:21

Topic	Vid Count	Duration	Courses	Duration
Security Awareness	45	02:18:39	17	05:49:00
Threat Actors	23	01:09:32	7	02:34:00
CUI / PII	10	00:30:20	1	00:33:00
Compliance	7	00:33:21	1	00:33:21
Total	85	04:31:52	26	09:29:21



Growing Library - Basic to Expert



Basic Content

&

“Premium” Cyber Content + Compliance (Confidential Info & Insider Threat)

Coming: "Premium" On Demand Threat Notifications; "Super Premium" Content for Execs, Developers & Admin



Customizable Home Page



Why am I taking this training?

[Click here to find out more!](#)



How do I take this training?

[Click here to find out more!](#)



Security This Week!

[Click here to listen to the latest podcast.](#)



The Latest Cyber Threats

[Click here to find out more!](#)

My Cyber Training

My Learning Campaigns

Incomplete Complete



My Stats



0
Total Points
Earned



0
Rank



N/A
Most Used
Feature



0
View Streak



Sample of Phishing Training

PULSAR ACCELERATORS Home Library Webinars Requests Author Skill Builder Schedule Coaching Search Keywords Feedback

Library / Cybersecurity

Combat Phishing Attempts for Organizations (Part 2)

From: nsd@nationalecurity.com **WARNING: PHISHING EMAIL DETECTED**

To: appleuser@mail.com

Subject: URGENT: Vulnerability Disclosure

National Security Department

A vulnerability has been identified in the Apple Facetime mobile application that allows an attacker to record calls and videos from your mobile device without your consent.

We have created a website for all citizens to verify if their videos and calls are safe to make public.

To perform the verification, please use the following link:

FACETIME VERIFICATION

Version: 3.0
Status: Public
Public: 12/20/2023
Skill Level: 0

Related Solutions

- Learn to Combat Phishing Attacks for Organizations (Skill Track) (Cybersecurity)
- Combat Phishing Attempts for Organizations (Part 1) (Cybersecurity)
- Combat Phishing Attempts for Organizations (Part 3) (Cybersecurity)
- Lesson: Combat Phishing Attacks for Organizations (Cybersecurity)
- List of Skill Tracks for Cybersecurity (Cybersecurity)

Attachments

No items found.

History

Compare Versions

v2 Modified: 12/20/2023 4:30:51 PM
v2 Modified: 12/20/2023 4:30:51 PM



Built-In Phishing Simulator / Activities

The screenshot displays an Outlook window titled "EmailPhishingDemo". The interface is in dark mode. On the left is the "Inbox" pane with a list of emails from various senders like Digital Federal Credit Union, Disney+, IT Admin, etc. The main pane shows an email from "dcu@dcu.org" with the subject "Important Tax Information for Your DCU Accounts". The email content features the DCU logo and a "GET STARTED" button. On the right is a "Scoring Panel" with three sections: "Sender", "Content", and "Links". Each section has "Seems Legit" and "Feels Phishy" buttons. A "Submit Selections" button is at the bottom of the panel.

Scenario: You have a Digital Federal Credit Union account.

Subject: Important Tax Information for Your DCU Accounts

dcu@dcu.org
To: Dean Dahlin

DCU

Important Tax Information for Your DCU Accounts

We wanted to let you know that all of your tax documents for your DCU accounts are now available.

Log into **Digital Banking** and click View Statements on the Membership tab to view and print your tax documents.

GET STARTED

220 Donald Lynch Boulevard
PO Box 9130
Marlborough, MA 01752-9130

ABA Routing Number:
211391825
SWIFT: 466914
Insured by NCUA

Our Privacy Policy protects your privacy and we will never sell your name or email address. Please do not reply to this email. For questions or additional information, please email dcu@dcu.org.

© 2023 Digital Federal Credit Union

Scoring Panel

Sender
Investigate who actually sent the email not just the name that is displayed.

Seems Legit Feels Phishy

Content
Examine the subject and body of the email for anything out of the ordinary.

Seems Legit Feels Phishy

Links
Check links before clicking to make sure their destination is what you expect and not somewhere malicious.

Seems Legit Feels Phishy

Submit Selections



Sample of Password Training

PULSAR
Home Library Webinars Requests Author Skill Builder Schedule Coaching Search Keywords

Library / Cybersecurity

Understand Effective Password Policies

Version: 3.0
Status: Public
Public: 3/21/2024
Skill Level: 0

Related Solutions

- List of Skill Tracks for Cybersecurity (Cybersecurity)
- Explore Effective Cybersecurity Policies (Skill Track) (Cybersecurity)
- Lesson: Explore Effective Cybersecurity Policies (Cybersecurity)
- Understand Effective Email Protection (Cybersecurity)
- Lesson: Understand BYOD Policies (Cybersecurity)

Attachments

No items found

History

Compare Versions

- v2 Modified: 01/17/2024 1:54:34 PM
- v2 Modified: 03/13/2024 1:58:10 PM
- v2 Modified: 03/21/2024 10:19:14 AM
- v2 Modified: 03/21/2024 10:24:17 AM
- v2 Modified: 03/21/2024 10:29:15 AM
- v2 Modified: 01/17/2024 1:54:34 PM

Do not enter passwords into your accounts when connected to public Wi-Fi!

Facebook login screen with a large red X over it.



Title	Category	Duration
Navigate Cybersecurity Learning Campaigns	Security Awareness	01:40
Why Am I Taking Cybersecurity Training?	Security Awareness	01:31
Password Management Introduction	Passwords & Authentication	01:19
Why is Password Management So Important?	Passwords & Authentication	02:42
Understand How Passwords are Compromised	Passwords & Authentication	03:15
What Makes a Weak Password	Passwords & Authentication	03:02
What Makes a Strong Password	Passwords & Authentication	03:37
Password Managers: One Password to Rule Them All	Passwords & Authentication	01:32
Password Management: Final Tips	Passwords & Authentication	02:10
Introduction to Phishing	Phishing	03:33
What Is Email Phishing	Phishing	02:20
How to Identify Phishing Emails	Phishing	03:54
Unique Categories of Phishing	Phishing	03:32
Recognize Phishing Attempts in Other Media Types	Phishing	03:27
Recognize Phishing Techniques	Phishing	01:40
Combat Phishing Attempts for Organizations (Part 1)	Phishing	02:41
Combat Phishing Attempts for Organizations (Part 2)	Phishing	01:53
Combat Phishing Attempts for Organizations (Part 3)	Phishing	02:01
What is a BYOD Policy?	USB/Removable Media	02:32
BYOD Security Risks	USB/Removable Media	05:20
Explore BYOD Security Measures (Part I)	USB/Removable Media	03:11
Explore BYOD Security Measures (Part II)	USB/Removable Media	05:05
Pros and Cons of USB Drives	USB/Removable Media	04:19
Explore Policy Options for USB Drives	USB/Removable Media	04:39
Explore Guidelines for USB Drives in the Workplace (Part 1)	USB/Removable Media	02:47
Explore Guidelines for USB Drives in the Workplace (Part 2)	USB/Removable Media	03:35
Understand the Importance of Security Awareness Training	Security Awareness	02:12
Know Thy Enemy (Pyramid of Threats)	Security Awareness	03:19



Title	Category	Duration
Understand the Insider Threat	Insider Threat	02:19
Learn the Categories of Insider Threats	Insider Threat	01:59
Meet the Unintentional Insider	Insider Threat	01:50
Meet the Intentional Insider	Insider Threat	02:03
Recognize the Risks for Insider Threats	Insider Threat	04:23
Combat Insider Threats	Insider Threat	03:34
Introduction to Artificial Intelligence (AI) and Cybersecurity	Insider Threat	02:50
Understand AI Terminology	AI Security	06:06
Understand the Hazards of AI	AI Security	04:55
Be a Protector, Not a Product	Social Media	01:35
Understand Social Media Risks Part 1	Social Media	02:25
Understand Social Media Risks Part 2	Social Media	02:50
Minimize Social Media Risks	Social Media	03:23
What is Cloud Computing	Social Media	04:01
Ensuring the Security of Software as a Service	Social Media	03:35
GDPR Basics Rights and Responsibilities	GDPR	05:29
GDPR Terminology	GDPR	04:09
Key Principles of GDPR	GDPR	04:34
Rights of GDPR Data Subjects Part 1	GDPR	05:35
Rights of GDPR Data Subjects Part 2	GDPR	04:42
GDPR Responsibilities of Organizations	GDPR	07:38
GDPR Conclusion	GDPR	01:14
Lock up the Backdoor of Remote Work	Remote Work	02:44
Ensure a Secure Network for Remote Work	Remote Work	04:16
Manage Devices for a Safe Remote Work Environment	Remote Work	03:44
Work Remotely with Confidence and Security	Remote Work	04:12
Identify the Types of Malware Part 1	Malware	04:42
Identify the Types of Malware Part 2	Malware	03:45
Defend Against External Threats Containing Malware	Malware	04:28
Stay Vigilant About Internal Threats Leading to Malware	Malware	02:46



Title	Category	Duration
Understand Effective Email Protection	Email	02:44
Understand Effective Password Policies	Email	02:17
Design Effective Physical Security for Organizations	Email	01:57
Understand Effective Password Policies	Passwords & Authentication	02:17
Understand Effective Email Protection	Passwords & Authentication	02:44
Design Effective Physical Security for Organizations	Passwords & Authentication	01:57
Practice Wireless Network Security	Network Security	04:01
Explore Basic and Advanced Client/Server Security	Network Security	02:20
Understand Essential Perimeter Security Components	Network Security	02:10
Understand IT Life Cycle and Patch Management	Network Security	02:18
Cybersecurity 101: Prepare For the Worst	Network Security	03:38
Introduction to the Ransomware Series	Ransomware	01:59
What Is Ransomware and How Is It Delivered?	Ransomware	03:55
Understand Who Sends Out Ransomware and Why	Ransomware	03:18
Identify Ransomware Phishing Emails	Ransomware	03:16
Identify Other Ransomware Vectors	Ransomware	02:46
Ways to Defend Against Ransomware (Part I)	Ransomware	03:43
Ways to Defend Against Ransomware (Part II)	Ransomware	03:50
??Introduction to Controlled Unclassified Information (CUI) Management	CUI	02:55
ISOO and DoD CUI: The Pillars of Protection	CUI	02:27
Explore Types of CUI	CUI	02:32
Get to Know Fundamental CUI Handling Principles and Stages (Part 1)	CUI	03:45
Get to Know Fundamental CUI Handling Principles and Stages (Part 2)	CUI	04:25
Comply with DoD Essential CUI Marking Guidelines	CUI	02:09
Safeguarding CUI: Comply with DoD Dissemination Controls and Markings	CUI	01:48
Simplify Portion Markings for CUI	CUI	01:42
Final Tips for CUI Handling	CUI	04:25