

Information Security

IT Partners
June 20, 2023

Jessica Murray

Information Security Officer

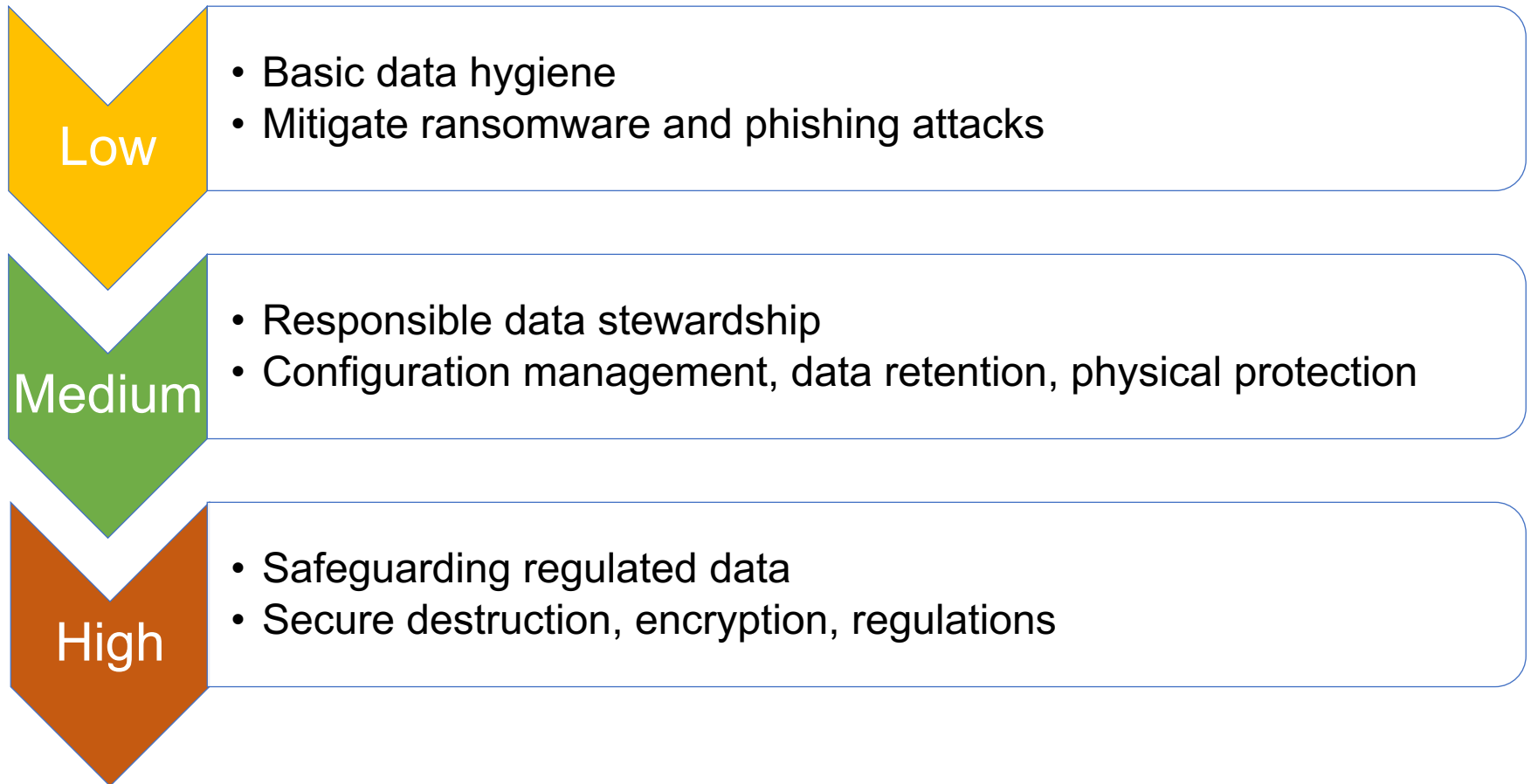
Information Systems & Technology

Outline

- Using Infoprotect – where can I store my data?
- Working toward NSPM-33 and NIST 800-171 compliance – 3 topics
 - Vulnerability Management
 - Remote Access
 - Security Awareness Training

InfoProtect.mit.edu: Data Classification

A flexible framework that enables DLCs to appropriately secure MIT information according to level of risk posed by loss of confidentiality, integrity or availability



Where can I store that?

- What risk level is the data?
- Review infoprotect.mit.edu tasks for Application and Server
- For Low and Medium Risk information – generally all centrally provided platforms are acceptable
- For High Risk information:
 - “Use file level encryption when sharing files on platforms like email, Dropbox, Slack. Encryption keys must be shared via another method.”
 - KB “Encrypting a file before Sharing” – Veracrypt, Cryptomator
 - Save the password in a password manager
- What about this free online survey tool?
- Consider the lifecycle of the data, what happens when people leave
- “Information Protection at MIT” course in Atlas

Remote Access

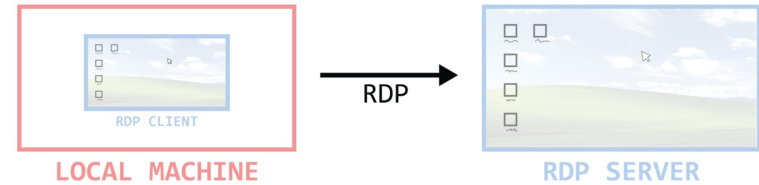


Figure 1: What is RDP?

- RDP, VNC, SSH, etc.
 - Remotely log in to a machine, via a console or graphical desktop. Could be a server on a public IP or a workstation within a private network
- Threats:
 - Vulnerabilities in protocols (Bluekeep)
 - RDP is the most popular initial ransomware attack vector
 - Insecure protocols – DDoS, poor encryption, etc
 - Password guessing/compromised credentials
- Retain cybersecurity insurance
 - Previous insurer actively scanned for RDP before renewal. Consistently comes up as a key issue.

Remote Access

NSPM-33

- Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.
- Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).
- Control any non-public information posted or processed on publicly accessible information systems

NIST 800-171

- Monitor and control remote access sessions.
- Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.
- Route remote access via managed access control points.
- Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts

Infoprotect

- Utilize multi-factor authentication for remote access.
- Utilize multi-factor authentication for remote interactive user and administrator logins
- Use vendor supported applications and operating systems.
- Do not reuse passwords for multiple services.
- Do not use your Kerberos password for non-Kerberos enabled system
- Information at this level is transmitted over an encrypted connection.

Remote Access Best Practices

- All systems patched
- Restrict remote access ports by IP via host firewall
 - MIT VPN ranges
- Use MFA (VPN also gets you this)
- Limit access by authorized user or group
- Research best practices for your solution
 - Most recent version, secure configuration
- Don't reuse passwords
- Jump Box

Vulnerability Management

NSPM-33

- Identify, report, and correct information and information system flaws in a timely manner.

NIST 800-171

- Identify, report, and correct system flaws in a timely manner.
- Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.
- Remediate vulnerabilities in accordance with risk assessments

Infoprotect

- Configure automatic download and application of software and operating system updates.
- Stay informed of available patches
- Perform regular network vulnerability scans. Contact your departmental IT administrator or security@mit.edu for assistance.

ALERT

CISA Adds New Vulnerability to Known Exploited Vulnerabilities Catalog

Cybersecurity and Infrastructure Security Agency

Known Exploited Vulnerabilities Catalog – List of vulnerabilities with a due date for remediation

Release Date: June 1, 2023

Common Vulnerabilities and Exposures
CVE ID - A unique, alphanumeric identifier

CISA has added one new vulnerability to its Known Exploited Vulnerabilities Catalog, based on evidence of active exploitation.

- [CVE-2023-3079](#) Google Chromium V8 T

These types of vulnerabilities are frequent a to the federal enterprise. **Note:** To view the "Date Added to Catalog" column

Binding Operational Directive BOD 22-01 – Requires Federal agencies to remediate vulnerabilities by the due date

pose significant risks click on the arrow in

[Binding Operational Directive \(BOD\) 22-01: Reducing the Significant Risk of Known Exploited Vulnerabilities](#) established the Known Exploited Vulnerabilities Catalog as a living list of known Common Vulnerabilities and Exposures (CVEs) that carry significant risk to the federal enterprise. BOD 22-01 requires Federal Civilian Executive Branch (FCEB) agencies to remediate identified vulnerabilities by the due date to protect FCEB networks against active threats. See the [BOD 22-01 Fact Sheet](#) for more information.

Example Known Exploited Vulnerability Bluekeep CVE-2019-0708

NIST Information Technology Laboratory
NATIONAL VULNERABILITY DATABASE

Severity CVSS Version 3.x CVSS Version 2.0

CVSS 3.x Severity and Metrics:
NIST: NVD Base Score: 9.8 CRITICAL
Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS v3.0 Severity and Metrics:
Base Score: 9.8 CRITICAL
Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Impact Score: 5.9
Exploitability Score: 3.9

Attack Vector (AV): Network
Attack Complexity (AC): Low
Privileges Required (PR): None
User Interaction (UI): None
Scope (S): Unchanged
Confidentiality (C): High
Integrity (I): High
Availability (A): High

Description
A remote code execution vulnerability formerly known as Terminal Services connects to the target system using RDP requests. aka 'Remote Desktop Service'

According to Microsoft, an attacker can send specially crafted packets to one of these operating systems that has RDP enabled. After successfully sending the packets, the attacker would have the ability to perform a number of actions: adding accounts with full user rights; viewing, changing, or deleting data; or installing programs. This exploit, which requires no user interaction, must occur before authentication to be successful. BlueKeep is considered “wormable” because malware exploiting this vulnerability on a system could propagate to other vulnerable systems; thus, a BlueKeep exploit would be capable of rapidly spreading in a fashion similar to the WannaCry malware attacks of 2017.

Checking Tenable Plugins

Known Exploited Vulnerability Bluekeep CVE-2019-0708

<https://www.tenable.com/plugins>

The screenshot shows the Tenable Plugins Search interface. The left sidebar contains navigation links: Plugins Pipeline, Newest, Updated, Search, Nessus Families, WAS Families, NNM Families, LCE Families, Tenable.ot Families, About Plugin Families, Nessus Release Notes, Audits, Tenable.cs Policies, and Tenable.ad. The main content area is titled 'Plugins Search' and includes a search bar with the text 'Start typing or add a filter...'. Below the search bar, there are filters for 'CVE (Active)' and 'Product(1)', with a 'Clear All' button. A 'Search by CVE' dropdown is open, showing 'CVE-2019-0708'. The search results are displayed in a table with columns: ID, Name, Product, Family, Published, Updated, and Severity. The results show three entries, all with a 'CRITICAL' severity. Two green callout boxes are overlaid on the image: one pointing to the search filters and another pointing to the search results table.

Filtered by CVE and Tenable Product (Nessus)

We can see what Plugins Tenable has available to detect this CVE

Plugins / Search

Plugins Search

Start typing or add a filter... Filter Relevance

CVE (Active) Product(1) Clear All

Search by CVE

CVE-2019-0708

Page 1 of 1 • 4 Total Next >>

ID	Name	Product	Family	Published	Updated	Severity
125313	Microsoft RDP RCE (CVE-2019-0708) (BlueKeep)(uncredentialed check)	Nessus	Windows	5/22/2019	5/31/2023	CRITICAL
125073	Microsoft Security Advisory 4500331: Guidance for older platforms (XP / 2003)(BlueKeep)	Nessus	Windows : Microsoft Bulletins	5/14/2019	12/5/2022	CRITICAL
125060	KB4499180: Windows Server 2008 and Windows Vista SP2 May 2019 Security Update (BlueKeep)	Nessus	Windows : Microsoft Bulletins	5/14/2019	12/5/2022	CRITICAL

Creating an Advanced Active Scan Policy

Using Tenable's Security Center

Known Exploited Vulnerability Bluekeep CVE-2019-0708

Add Policy > Advanced Scan

- Setup
- Advanced
- Host Discovery
- Port Scanning
- Service Discovery
- Assessment
- Brute Force
- Malware
- SCADA
- Web Applications
- Windows
- Report
- Authentication
- Compliance
- Plugins

Plugins

Showing both enabled and disabled items. [Hide Disabled](#)

Status	Plugin Family	Matched
MIXED 1	Windows	1
MIXED 3	Windows : Microsoft Bulletins	3

CVE ID ▾

Enter CVE ID

Update Filter

Clear Filter

[Lock All Mixed](#) / [Unlock All Mixed](#)

[Enable Shown](#) / [Disable Shown](#)

Using the Policy to Create an Active Scan

Using Tenable's Security Center

Known Exploited Vulnerability Bluekeep CVE-2019-0708

Add Active Scan

- General
- Settings
- Targets
- Credentials
- Post Scan

General

NAME *

DESCRIPTION

POLICY *

Schedule

SCHEDULE On

- Basic Network Scan (aggressive discovery)
- Basic Network Scan Debug
- BlueKeep CVE-2019-0708 ⓘ
- CISA alert aggressive
- CISA alert unmodified
- CISA Alerts

Cancel

Submit

Using Tenable's Security Center Searching Scan Results Known Exploited Vulnerabilities non-IS&T

Vulnerability Summary

Vulnerability Summary ▼

Mitigated

Cumulative

Vulnerabilities

Queries

Events

Mobile



456 Result(s)

[Jump to Vulnerability Detail](#) [Export](#) [Save](#) [More](#)

1 to 50 of 456

Page 1 of 10

<input type="checkbox"/>	Plugin ID	Name	Family	Severity	VPR	Total
<input type="checkbox"/>	125131	Oracle WebLogic Java Report Deserialization (CVE-2019-3804)	Web Servers	HIGH	9.8	9
<input type="checkbox"/>	125132	Apache Struts 2.3.33-2.3.39 Remote Code Execution (CVE-2019-0199)	Web Servers	MEDIUM	6.7	3
<input type="checkbox"/>	125133	Tomcat PDF Manager Remote Code Execution (CVE-2019-0200)	CGI abuses	HIGH	9.2	2
<input type="checkbox"/>	125134	Apache Struts 2.3.33-2.3.39 Remote Code Execution (CVE-2019-0199)	Web Servers	HIGH	7.4	9
<input type="checkbox"/>	125313	Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (unc...)	Windows	CRITICAL	9.7	2
<input type="checkbox"/>	125135	Oracle WebLogic Java Report Deserialization (CVE-2019-3804)	Misc.	MEDIUM	7.4	3
<input type="checkbox"/>	125136	Red Hat Local Security Checks (CVE-2019-0200)	Red Hat Local Security Checks	MEDIUM	4.4	3
<input type="checkbox"/>	125137	Apache Struts 2.3.33-2.3.39 Remote Code Execution (CVE-2019-0199)	CGI abuses	MEDIUM	3.6	1
<input type="checkbox"/>	125138	Red Hat Local Security Checks (CVE-2019-0200)	Red Hat Local Security Checks	MEDIUM	6.7	3
<input type="checkbox"/>	125139	Apache Struts 2.3.33-2.3.39 Remote Code Execution (CVE-2019-0199)	Web Servers	HIGH	9.0	37
<input type="checkbox"/>	125140	Red Hat Local Security Checks (CVE-2019-0200)	Red Hat Local Security Checks	HIGH	6.7	3

Vulnerability Scanning with Tenable Security Center

- Network Vulnerability Scanning (Nessus)
 - Static IPs
- Request an account from security@mit.edu.
 - List of Kerberos IDs of those needing to scan
 - List of IP addresses they should have access to scan
- KB: Vulnerability Scanning with Tenable Security Center at MIT
- Subscribe to CISA alerts and updates to the Known Vulnerabilities List on the CISA website

Security Awareness Training

NSPM-33

- Provide regular cybersecurity awareness training for authorized users of information systems, including in recognizing and responding to social engineering threats and cyber breaches
- Provide training to relevant personnel on research security threat awareness and identification, including insider threat training where applicable.... In addition to periodic training, research organizations should conduct tailored training in the event of a research security incident.

NIST 800-171

- Ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.
- Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities.
- Provide security awareness training on recognizing and reporting potential indicators of insider threat.

Infoprotect

- Train all users with access to ensure understanding of their responsibilities with regard to handling information.
- Train all users with access to ensure awareness of the risks to information and data

Security Awareness Training Resources – SANS Courses

- Available in Atlas under “Community Safety & Security”
- Awareness I: IT Security
 - Understanding common security risks, social engineering, email attacks, password protection, mobile device safety, and hacking.
- Awareness II: IT Security
 - How to enhance your cyber security when working remotely, traveling internationally, using social networks, and handling Personal Identifiable Information (PII) as well as Federal Personally Identifiable Information (FPII). It will also provide you with opportunities to practice your knowledge on the topics covered.
- Can be assigned to your dept, contact training@mit.edu

COMMUNITY SAFETY & SECURITY

10 Community Safety

20 Information Security

Awareness I: IT Security ★ Learning Bundle

Awareness II: IT Security 🖥️ Web-Based

Client Confidentiality in Law Offices 🖥️ Web-Based

Cloud Services 🖥️ Web-Based

Criminal Justice 🖥️ Web-Based

EU General Data Protection Reg. (EUGDPR) 🖥️ Web-Based

Federal Tax Information 🖥️ Web-Based

FERPA 🖥️ Web-Based

Security Awareness Training Resources – KnowBe4 Library

- Available at training.knowbe4.com
- Login with Kerberos
- Click on Name in upper right and choose “My Training”
- Security Awareness Foundations (25 min)
- Phishing Foundations (15 min)

The screenshot displays the KnowBe4 training library interface. At the top left is the MIT Massachusetts Institute of Technology logo. Navigation links for 'Dashboard', 'Training', and 'Library' are visible. The user's name, 'Jessica Murray', is shown in the top right corner with a dropdown menu containing options: 'My Training', 'Profile', 'Account Settings', 'Return to Console', 'Go to PhishER', 'Log Out', and 'English (United States)'. The main content area features a heading 'Continue learning with the optional training content below.' Below this is a search bar with a 'Content Types' dropdown set to 'All' and a search input field. The 'Continue Learning' section displays two identical training module cards. Each card has a thumbnail image of hands forming a circle, an 'In Progress' status indicator, the title 'Security Awareness Foundations', and a 'Training Module' icon.

Security Awareness Training Phishing Simulations with KnowBe4

- Specify group
- Duration
- Template Category
- Randomize Templates
- Difficulty
- Landing Page
- Track “Clickers”

Note: A campaign will start 10 minutes after it is activated or created.

Campaign Name: IS&T Quarterly

Send to: All Users | **Specific Groups** ⓘ
ist-kb4-staff X

Frequency: One-time | Weekly | Biweekly | Monthly | **Quarterly** ⓘ

Start Time: 06/15/2023 | 12:24 PM | (GMT-05:00) Eastern Time (US & Canada)

Sending Period: Send all emails when the campaign starts ⓘ
 Send emails over 3 business days ⓘ

Define Business Days and Hours Using Time Zone: (GMT-05:00) ⓘ
9:00 AM to 5:00 PM
 Sun Mon Tues Wed Thur Fri Sat

Track Activity: 3 days after the sending period ends ⓘ
 Track Replies to Phishing Emails ⓘ

Template Categories: IT X | Full Random (Random email to each user) ⓘ [Preview](#)

Send Localized Emails ⓘ

Difficulty Rating: ★★★★★- Advanced ⓘ

Phish Link Domain: Random Domain ⓘ

Landing Page: Jess Classic: SEI Landing Page (Translatable) (...) ⓘ

Add Clickers to: Select Group ⓘ

Send an email report to account admins after each phishing test

Security Awareness Training

Phishing Simulations with KnowBe4

One of these is from KnowBe4

Your mailbox is almost full. None X

This message was sent with High importance.

Microsoft Outlook
To: Jessica Murray
Mon 6/19/2023 8:02 PM

Your mailbox is almost full.

98 GB 99 GB

To make room in your mailbox, delete any items you don't need and empty your mailbox. Learn more about [storage limits](#).

Mailbox address:
jlmurray@mit.edu

Reply Forward

Spam Notification: 1 New Messages None X

Some content in this message has been blocked because the sender isn't in your Safe senders list. [I trust content from quarantine@alerts-microsoft.com](#). | [Show blocked content](#)

Message Services <quarantine@alerts-microsoft.com>
To: Jessica Murray
Mon 6/19/2023 4:48 PM

[Microsoft 365 Logo](#)

Dear jlmurray@mit.edu:

You have 1 new spam-quarantined messages as of Wednesday 12:00 AM (UTC) which are listed below along with the actions that can be taken:

Release to Inbox: Send the message to your Inbox.

Report as Not Junk: Send a copy of the message to Microsoft for analysis.


Sender	Subject	Date (UTC)	Size	Release	Report
"Amazon.com" <shipment-tracking@amazon.com>	Your Amazon.com order of...	Wednesday 4:42 PM	64730	Release to Inbox	Report as Not Junk


© 2017 Microsoft Corporation. All rights reserved. | [Acceptable Use Policy](#) | [Privacy Notice](#)

Security Awareness Training

Phishing Simulations with KnowBe4

Sample landing page

 **Massachusetts
Institute of
Technology**


 English - United States

Oops! You clicked on a simulated phishing test!

Please review the Social Engineering Indicators found in the email you clicked on.
Remember to report any suspicious emails to phishing@mit.edu

Hover over the red flags to see details:

From: Message Services <quarantine@alerts-microsoft.com>
Reply-to: Message Services <quarantine@alerts-microsoft.com>
Subject: Spam Notification: 1 New Messages



Dear jlmurray@mit.edu:

You have 1 new spam-quarantined messages as of Wednesday 12:00 AM (UTC) which are listed below along with the actions that can be taken:

Release to Inbox: Send the message to your Inbox.

Report as Not Junk: Send a copy of the message to Microsoft for analysis.

Hover over the link. Link does not take you to the site the email content says it will.

Sender	Subject	Date (UTC)	Size	Actions
"Amazon.com" <shipment-tracking@amazon.com>	Your Amazon.com order of...	Wednesday 4:42 PM	64730	Release to Inbox Report as Not Junk

© 2017 Microsoft Corporation. All rights reserved. | [Acceptable Use Policy](#) | [Privacy Notice](#)

Report Phishing with the Phish Alert Button

KB: Reporting Phishing Email

The screenshot displays the Microsoft Outlook interface. The main window shows an email from Amazon titled "Kindle deals under \$5 on books by these authors". The email content includes a promotional message: "Here are some limited-time book deals picked just for you" and a section titled "Kindle deals for you" with a link to "See all Kindle deals >".

On the right side of the Outlook window, a "Phish Alert" sidebar is open. It features a blue header with "M365" and "IS&T Security Team". The text asks, "Are you sure you want to report this as a phishing email?". Below this, the "Subject" is listed as "Kindle deals under \$5 on books by...". There is a "Show Sender's Details" link and an "Email Classification" section with three radio button options: "Phish/Suspicious" (selected), "Spam", and "Unknown". At the bottom of the sidebar, a blue button labeled "Report Phishing" is highlighted with a red rectangular box.

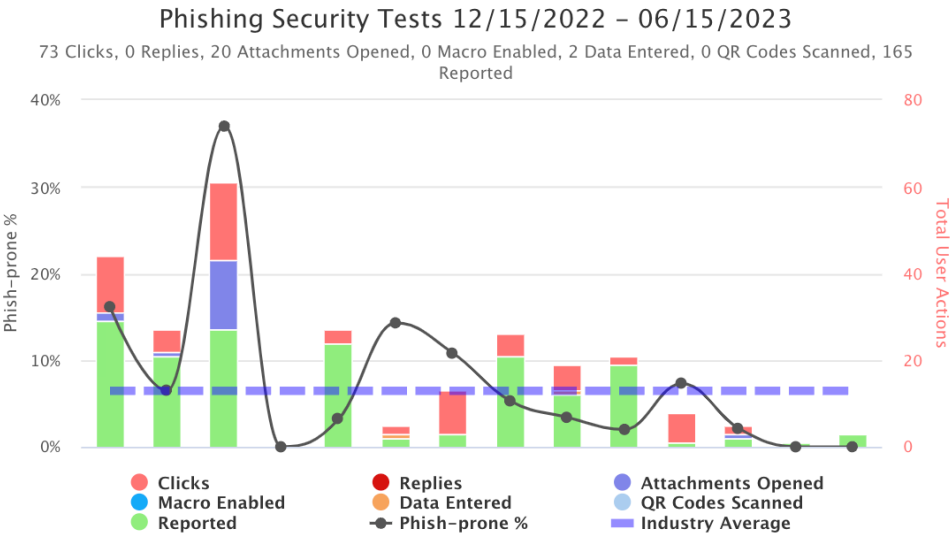
The Outlook ribbon at the top includes tabs for "Home", "Organize", and "Tools". The "Home" tab is active, showing various email management icons like "New Email", "Delete", "Reply", "Forward", and "Move". The "Phish Alert" icon is visible in the top right corner of the ribbon.

Security Awareness Training

Phishing Simulations with KnowBe4

Viewing phishing campaign results

205 Recipients	100% 205 Delivered	61% 125 Opened	2.9% 6 Clicked	0% 0 QR Code Scanned	0% 0 Replied	0% 0 Attachment Opened	0% 0 Macro Enabled	0.5% 1 Data Entered	5.9% 12 Reported	0% 0 Bounced
--------------------------	---------------------------------	-----------------------------	-----------------------------	-----------------------------------	---------------------------	-------------------------------------	---------------------------------	----------------------------------	-------------------------------	---------------------------



If folks use the Phish Alert Button, it will show up as "reported" in the stats and they will also receive immediate feedback that they reported a phishing campaign

Security Awareness Training Training Campaign with KnowBe4

Create New Training Campaign

[← Back to Training](#)

Campaign Name

Start Date

(GMT-05:00) Eastern Time (US & Canada)

End Date

Select Date and Time

Allow assignments to be completed after due date

[Visit ModStore](#)

Select one or more items from the list...

Enable Content Survey

Allow users to leave comments

Track Scores

Enroll Users

[View All Groups](#)

Select one or more groups from the list...

Enroll with CSV File


Enable automatic enrollment for new users

Enable progress reset for remedial training



Choose the group – can use the “Clickers” group from a phishing campaign

Choose the content – many courses available in the KnowBe4 ModStore

Security Awareness Training Training Campaign with KnowBe4

 **Massachusetts Institute of Technology**

DASHBOARD PHISHING TRAINING SECURITYCOACH **New** USERS ASAP PHYSICAL TESTS ▾ SECOND CHANCE **MODSTORE** REPORTS

jlmurray@mit.edu  

ModStore Browse Library Brandable Content Uploaded Content

#1 USED CONTENT

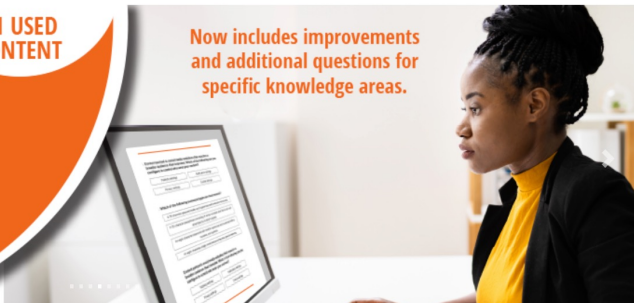
Featured Content

Security Awareness Proficiency Assessment

Assessment | 10 minutes | July 2022

[View Details](#) [Add to Library](#)


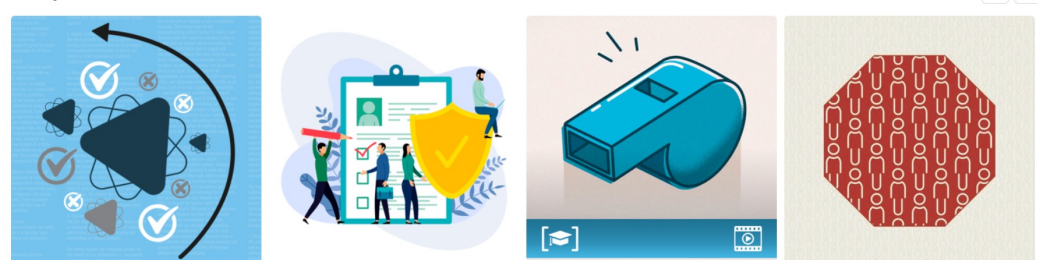
Now includes improvements and additional questions for specific knowledge areas.



Content Types: All ▾ Topics: All ▾ Search: Search 🔍

Additional Filters +

Compliance Plus Essentials



Security Awareness Training

Getting Started with KnowBe4

- KB “DLC phishing and security awareness training”
Create two moira groups with the following naming convention
 - admin group = dlcname-kb4-admins, e.g. meche-kb4-admins
 - user group(s) = dlcname-kb4 or dlcname-kb4-subgroup for each user list or sublist, e.g. meche-kb4 or meche-kb4-faculty
- Groups can be nested lists of existing groups if desired
- Submit a ticket to servicedesk@mit.edu
 - Request Knowbe4 access from Information Security
 - Include the admin group name and the user group name

Questions?