DREXEL CYBERSECURITY INCIDENT RESPONSE

Tashnuva Chowdhury, Diya Patel, Kristi Kesslick, Owen Gambo, Siddarth Kampalli

Our Objective

This project simulates Drexel University's Information Security team by developing an incident response and risk management framework for a higher education environment. The goal is to create a structured process for identifying, containing, and resolving cybersecurity incidents affecting university systems, accounts, and data, with a focus on threats such as phishing, malware, and compromised accounts.

Statement of Work

The purpose of this project is to design a structured incident response and risk management framework, which is tailored to Drexel University's digital environment

Severity Classifications

How risk is calculated for an incident

Likelihood Levels

Likelihood Level Definitions		
Level	**Likelihood**	**Definition**
1 - Rare	<5% annual probability (≤1 occurrence every 20+ years)	No historical precedent; strong controls; low threat exposure
2 - Unlikely	5–20% annual probability (1 every 5–20 years)	Seen in higher ed sector but not at institution
3 - Moderate	20–50% annual probability (1 every 2–5 years)	Occurs in peer institutions (phishing credential compromise)
4 - Likely	50–80% annual probability (1+ per year expected)	Common in higher ed (ransomware attempts, account takeovers)
5 - Certain	>80% annual probability (multiple times per year)	Actively occurring (phishing campaigns, vulnerability scans)

Impact Criteria

Likelihood Level Definitions		
Level	**Likelihood**	**Definition**
1 - Rare	<5% annual probability (≤1 occurrence every 20+ years)	No historical precedent; strong controls; low threat exposure
2 - Unlikely	5–20% annual probability (1 every 5–20 years)	Seen in higher ed sector but not at institution
3 - Moderate	20–50% annual probability (1 every 2–5 years)	Occurs in peer institutions (phishing credential compromise)
4 - Likely	50–80% annual probability (1+ per year expected)	Common in higher ed (ransomware attempts, account takeovers)
5 - Certain	>80% annual probability (multiple times per year)	Actively occurring (phishing campaigns, vulnerability scans)

Risk Matrix

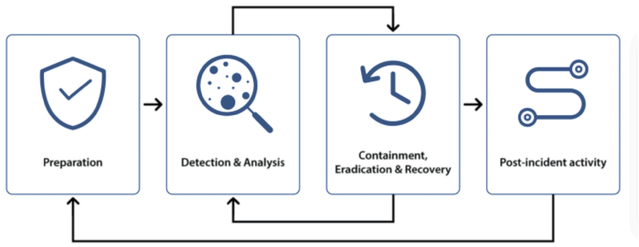
	IMPACT →				
LIKELIHOOD ↓	Insignificant 1	Minor 2	Significant 3	Major 4	Severe 5
1 Rare	LOW 1	LOW 2	LOW 3	MEDIUM 4	MEDIUM 5
2 Unlikely	LOW 2	MEDIUM 4	MEDIUM 6	HIGH 8	HIGH 10
3 Moderate	LOW 3	MEDIUM 6	HIGH 9	HIGH 12	EXTREME 15
4 Likely	MEDIUM 4	HIGH 8	HIGH 12	EXTREME 16	EXTREME 20
5 Certain	MEDIUM 5	HIGH 10	EXTREME 15	EXTREME 20	EXTREME 25

Risk Score = Likelihood x Impact

Acknowledgments

We would like to thank Emanuel Lazar and the Drexel University Security Team for their guidance and support throughout this project. We greatly appreciate the opportunity to learn from their expertise and mentorship.

NIST Incident Response Cycle



The NIST Incident Response Lifecycle is a step-by-step framework used to go through the steps from identifying to closing incidents.

Standard Operating Procedure

	Standard Operating Procedure - Phishing Incident Response	**Document ID:** SOP.RR.002 **Document Version:** 1.0 **Approved By:** Drexel University Incident Response Team **Revision Date:** 3/11/2026

We created Standard Operating Procedures (SOPs) for the following:

- Phishing Incidents
- Compromised Accounts Incidents
- Malware Incident
- Risk Response Plan

Security Awareness & Training Plan

The plan establishes preventive security education tailored to students, staff, and administrative users, addressing common threats such as phishing, malware, weak passwords, and compromised accounts. It defines training topics, delivery methods, training frequency, effectiveness measurements, and continuous improvement procedures to strengthen the university's overall security posture and reduce future incidents.

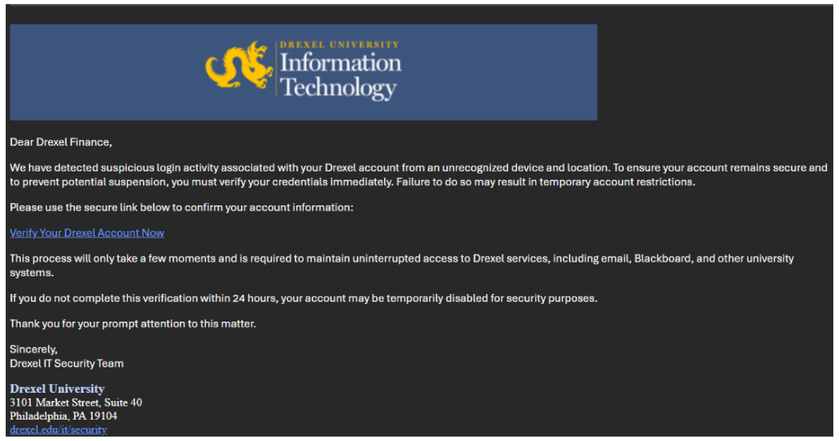
Phishing Incident Example

Sprint 8: Final Incident Simulation & Report

1. Introduction

1.1 Purpose

The purpose of this report is to document the identification, analysis, response, and resolution of a simulated phishing incident within the Drexel University environment. This report demonstrates the application of a structured incident response framework, including detection, triage, severity classification, containment, remediation, recovery, and post-incident review. The goal is to illustrate how Drexel IT Services and Security Operations Center (SOC) respond to a real-world phishing incident using standardized procedures and security controls.



DREXEL UNIVERSITY Information Technology

Dear Drexel Finance,

We have detected suspicious login activity associated with your Drexel account from an unrecognized device and location. To ensure your account remains secure and to prevent potential suspension, you must verify your credentials immediately. Failure to do so may result in temporary account restrictions.

Please use the secure link below to confirm your account information:

Verify Your Drexel Account Now

This process will only take a few moments and is required to maintain uninterrupted access to Drexel services, including email, Blackboard, and other university systems.

If you do not complete this verification within 24 hours, your account may be temporarily disabled for security purposes.

Thank you for your prompt attention to this matter.

Sincerely,
Drexel IT Security Team

Drexel University
3101 Market Street, Suite 40
Philadelphia, PA 19104
drexel.edu/it/security

1.2 Scope

This incident involves a phishing attack targeting a Drexel University employee in the Finance Office, which led to the compromise of university credentials and attempted unauthorized access across Drexel's integrated systems.

The scope of this incident includes the following Drexel-managed systems and components:

- Drexel Email System (Microsoft 365 / Exchange Online)
  - Used as the initial attack vector through a spoofed Drexel IT Services phishing email.
- User Account Credentials (Drexel Single Sign-On / Identity Management System)
  - Compromised credentials used to attempt authentication into multiple Drexel services including DrexelOne and administrative portals.
- Internal File-Sharing and Collaboration Platforms
  - Includes Drexel-managed SharePoint and OneDrive environments containing departmental and financial documents.
- Security Monitoring and Logging Infrastructure (Drexel SOC Tools)
  - Includes SIEM systems, identity monitoring tools, and Microsoft Defender for Office 365 used to detect anomalous login behavior, suspicious email activity, and potential lateral movement attempts.

Phishing Analysis Workflow