Worthington School District ISD #0518 Cyber Incident Report

Date: 03/09/2022

Name of individual completing this form: SWWC Cyber Security Team

Tracking number: 0001

Incident Priority

☐ HIGH	☐ MEDIUM	☒ LOW	☐ OTHER
Additional notes: Incident has been organized as a Low priority due to it being a user password compromise. Due to the user that was compromised and items that person had in their mailbox the priority level is located at the higher end of low close to becoming a medium incident			

Incident Type

Check all that apply.

☐ Compromised System	☐ Lost Equipment/Theft
☒ Compromised User Credentials (e.g., lost password)	☐ Physical Break-in
☐ Network Attack (e.g., DoS)	☒ Social Engineering (e.g., Phishing)
☐ Malware (e.g., virus, worm, Trojan)	☐ Law Enforcement Request
☐ Reconnaissance (e.g., scanning, sniffing)	☐ Policy Violation (e.g., acceptable use)
	☐ Unknown/Other (Please describe below.)
Incident description notes: User account was compromised and used to send out 754 phishing emails across a multitude of different email addresses.	

Incident Timeline

Please provide as much detail as possible.

A. Date and time when the incident was discovered	02/28/2022 at 11:05 A.M. CST
B. Date and time when the incident was reported	02/28/2022 at 10:40 A.M. CST
C. Date and time when the incident occurred	With limited Logging only going back to December 1, 2021, first external access from Nigeria came was successful on February 15, 2022 at 2:27 P.M. CST. With phishing emails not being sent out till February 28, 2022.

Additional timeline details:

Monday February 28th, 2022

10:32 – Phishing emails started to be sent out via ISD518 email account
11:05 – SWWC Cybersecurity was notified of phishing emails being sent out
11:29 – ISD518 staff informed SWWC Cybersecurity that he was looking into the phishing emails
11:38 – Affected user Active Directory account was fully disabled
11:48 – Phishing website was blocked in the firewall
12 P.M- User account was then updated with a new password and MFA was turned on
12:15 – Phishing email was tested by SWWC Cybersecurity
12:30 – Phishing websites were reported to FlipHTML5 and Cloudflare
3:07 – Next steps were discussed with ISD518 IT Director and SWWC Cybersecurity
4:30 – Recommendation email sent from SWWC Cybersecurity to ISD518 IT Director

Tuesday March 1, 2022
– Contact was made with FRSecure and meeting was set
– SWWC Cybersecurity and Worthington Technology Department met with FRSecure
Wednesday March 2, 2022
– Meeting with SWWC Cybersecurity and Worthington took place
– SWWC Cybersecurity collected full audit logs and started full investigation
Thursday March 3, 2022
- SWWC Cybersecurity continued their review of the Office 365 audit logs
- Worthington technology was informed that nothing had been found yet in the log files
Monday March 7, 2022
- SWWC Cybersecurity finalized their report and notified Worthington technology department. SWWC Cybersecurity concluded that with logs collected there did not appear to be any downloading, forwarding, or reading of staff member's email. SWWC Cybersecurity would like to note that some log/audit files are limited to only 7 days so SWWC Cybersecurity can't say without a doubt that affected email was not downloaded, forwarded, or read in the days before February 23, 2022.

Incident Scope

Please provide as much detail as possible.

A. Estimated quantity of systems affected	1
B. Estimated quantity of users affected	1
C. Third parties involved or affected (e.g., vendors, contractors, partners)	Microsoft Office 365
Additional scoping information: With the logs pulled from Office365, it doesn't appear that the intruder accessed anything other than Office 365 with a focus on Exchange Online.	

Systems Affected by the Incident

Please provide as much detail as possible.

A. Attack sources (e.g., IP address, port)	105.112.70.97 Nigeria 197.210.85.9 Nigeria 197.210.85.222 Nigeria 105.112.31.15 Nigeria 105.112.189.227 Nigeria
B. Attack destinations (e.g., IP address, port)	ISD518 User Office 365 Account
C. IP addresses of the affectedsystems	N/A
D: Primary functions of the affected systems (e.g., web server, domain controller)	Document Storage and Exchange Online
E. Operating systems of the affected systems (e.g., version, service pack, patch level, configuration)	Office 365
F. Security software loaded on the affected systems (e.g., anti-virus, anti-spyware, firewall, versions, date of latest definitions)	N/A
G. Physical location of the affected systems (e.g., state, city, building, room, desk):	Microsoft Data Center
Additional details:	

Users Affected by the Incident

Please provide as much detail as possible.

A. Names and job titles of the affected users:	ISD518 User Worthington District School Educator
B. System access levels or rights of the affected user (e.g., regular user, domain administrator, root)	Regular User – No special access
Additional user details:	

Incident Handling Log

Please provide as much detail as possible.

A. Actions taken to identify the affected resources	Office 365 Audit logs retained and reviewed Password not used with any other accounts
B. Actions taken to remediate the incident	Account disabled Account password changed MFA enabled for Account Phishing websites blocked in firewall
C. Actions planned to prevent similar incidents	District looking into 3rd party MFA provider Looking into conditional access within Azure Password policy review
Additional remediation details:	

Incident Declaration Criteria

Cybersecurity incidents are to be declared and qualified as high, medium, or low when they meet the following criteria. Incidents are to be declared based on an assessment of the gravity of the situation, criticality of the service impacted, sensitivity of information threatened or compromised, and potential for harm to this organization.[65]

Outlined below are potential specific criteria for each of the classes (High, Medium, and Low) of cybersecurity events. This list is not all-inclusive and should be tailored to your operating environment.

1. *HIGH-LEVEL CYBERSECURITY INCIDENTS*

High-level cybersecurity incidents are disruptions that are the most serious and are considered significant. Because of the gravity of the situation and the high potential for harm to the organization, these incidents should be handled immediately. Incidents that should be classified as "High" include events, activities, and violations such as possibly life-threatening activity, compromise of critical systems or information, root compromise, child pornography, pornographic trafficking, unauthorized music/software trafficking, and any violation of law or statute.

Incidents classified as "High" include

- suspected computer or network break-in
- website defacements or compromises, including failure to take the website offline or deregister the URL when the website is no longer used or supported by the organization
- successful denial-of-service (DoS) attacks by the organization's cyber resources or against the organization's cyber
  resources
- computer virus/worms/Trojan horses for which anti-virus software updates are not available or their deployment will be delayed
- detection of malware, including viruses, worms, Trojan horses, or spyware caused by employees who have declined to bring laptops into the office for upgrades
- connection of nonorganizational computers and servers to the organization's network without authorization or in violation of security policies
- unauthorized use of a system for processing or storing nonorganizational or prohibited data or information on organizational cyber resources, including the establishment and operation of a private or personal business
- changes to system hardware, firmware, or software without the system owner's authorization
- property destruction related to a cybersecurity incident (exceeding $100,000)
- personal theft related to a cybersecurity incident (exceeding $100,000)
- electronic file transfer (EFT) exploitation/manipulation or engaging in phishing or pharming
- installation, use, or sharing of peer-to-peer software
- activity including unauthorized or illegal serving out, downloading, or sale of copyrighted material
- child pornography
- pornography
- online gambling

- attempts to circumvent access to any organizational blocked websites such as pornography, gambling,and hate crimes
- download, use, or sharing of copyright-protected music or unauthorized software
- misuse of organizational property, facilities, or services, including accepting payment or services toprovide access to or use of organizational cyber resources in excess of one's authority
- any violation of the law

2. *MEDIUM-LEVEL CYBERSECURITY INCIDENTS*

Medium-level cybersecurity incidents are potentially serious and should be handled the same day that theincident occurs or that notification of the incident is given.

Incidents classified as "Medium" include

- adverse action resulting in employee termination in which the organization's cyber resources are neitherthe tool or target of the action
- Intrusion Detection System (IDS) reports that define activity as medium
- unauthorized use of a system for processing or storing organizational data
- property destruction related to a cybersecurity incident (less than $100,000)
- personal theft related to a cybersecurity incident (less than $100,000)
- misuse of organizational property, facilities, and services
- unconfirmed computer virus/worms (depending on impact to business unit and if the infection is theresult of a security policy violation)
- undocumented or unapproved vulnerability scans

3. *LOW-LEVEL CYBERSECURITY INCIDENTS*

Low-level cybersecurity events are the least severe and should be investigated no more than three workingdays after the incident occurs.

Incidents classified as "Low" include

- loss or compromise of a personal password
- suspected sharing of individually assigned accounts
- minor misuse of organizational property, facilities, and services
- unsuccessful scans/probes (internal and external)
- detected computer virus/worms (depending on impact to business unit)