

# So You've Been Hacked



Orion Township  
Public Library

Chase McMunn  
James Pugh  
Steve Saunders

# Bio Page



Chase McMunn - Director, Orion Township Public Library



James Pugh - Director, Cedar Springs Public Library  
*was the Community Relations Specialist at time of Cyberattack*



Steve Saunders - Head of IT, Orion Township Public Library



# Today we will...

- Tell you the story of how we were hacked, and lived to tell the tale
- Talk about our response to being hacked
- Explain what we actually should have done
- Hopefully leave you with some advice so you don't have to learn the hard way



# Learning Outcomes

1. Know some of the best practices to secure your network from a cyberattack
2. Know the first steps to take if your library is the target of a cyberattack
3. Be able to communicate with community stakeholders about the process



# The ~~Incident~~ Hackening - Day 1

Friday, October 20, 2023

1. A small collection of documents were reported inaccessible
2. A rogue script found actively running on a virtual server
3. The host server was rebooted by staff to stop any active processes
4. IT Consultant was contacted
5. External network communication severed by staff
6. Initial assessment and password resetting began



# The Villains Revealed!



**YOUR NETWORK INFECTED!**  
**ALL YOUR FILES ENCRYPTED**  
**AND HAS BEEN STOLEN!**

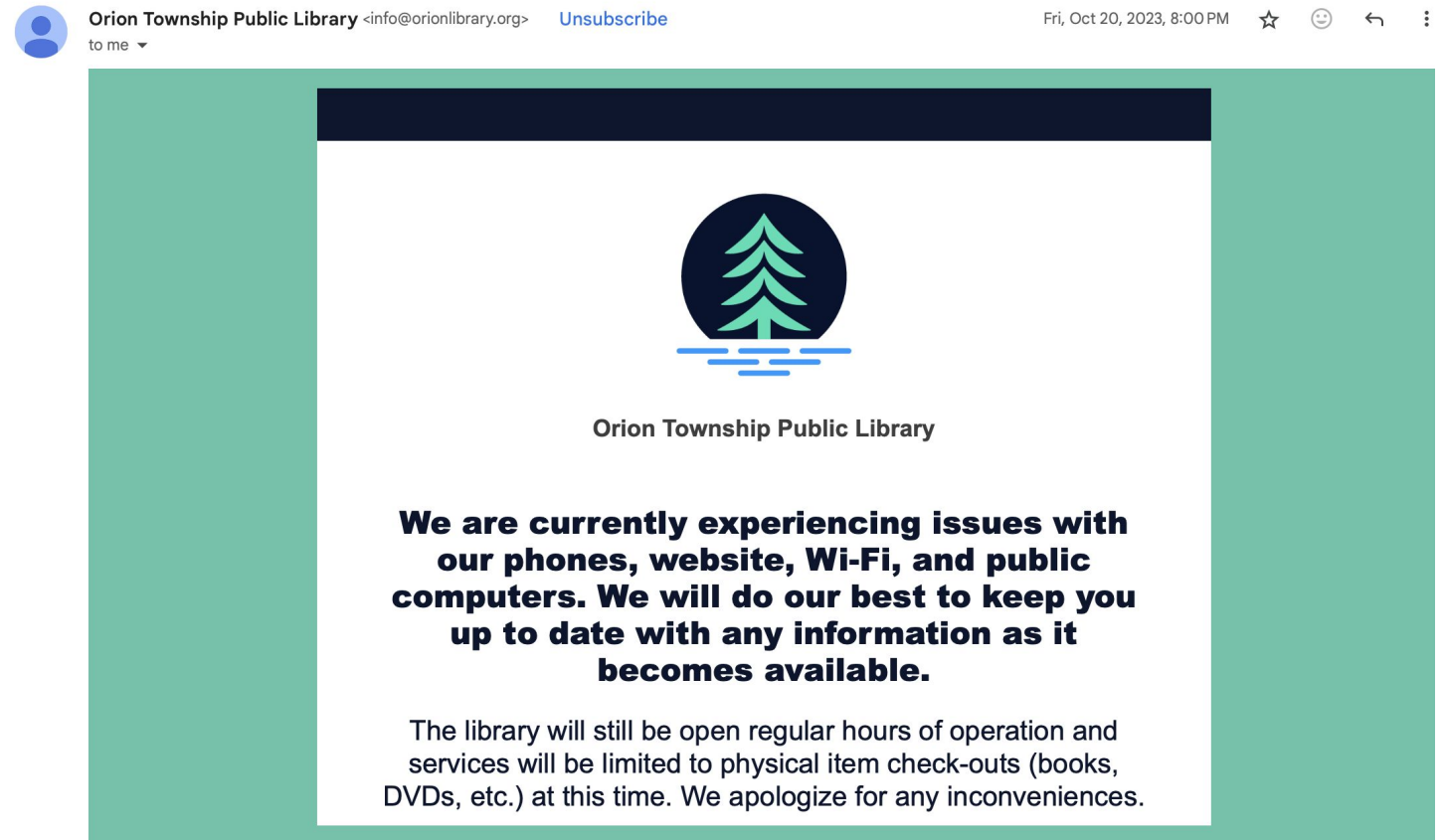
for details see **HOW\_TO\_RECOVER\_FILES.TXT**  
don't try modify encrypted files at yourself!!!



# First email

Sent out an email about the outage the evening of October 20, 2023.

Treated the issue as an outage, not an attack



# The ~~Incident~~ Hackening - Day 2

Saturday, October 21, 2023

IT Consultants arrived onsite to perform a thorough inspection of the network and devices.

## **The Bad**

- 8 VMs across 2 Physical Hosts infected
- Onsite Backups Deleted

## **The Good (or Lucky)**

- Staff / Public Workstations and ILS unaffected
- Backups were recoverable





# Crisis Communication

Sent out an email and social media post on October 25, 2023

- Told the truth
- Told it first
- Shared everything we knew at the time
- Said it fast
- Told people who matter most

Reassured patron info was safe



Orion Township Public Library

## Technical Issues Update

Over the weekend of October 20, 2023, the library experienced a malware attack on our servers. This was discovered quickly, and we have been working to safely bring our servers back online.

Most issues with our servers have been resolved as of October 25, 2023. Most services are available, including public Wi-Fi, access to the Internet, all materials can be checked out, and public printing. Our website is also up and running. Some online resources such as Oakland County Historical Resources may not work properly, we are still working to restore those features. If you notice any additional technical issues, please let us know.

**We would like to reassure patrons that no personal data was compromised in this past weekend's malware attack.**

We thank you for your patience and understanding with this issue. Please feel free to contact us at 248-693-3000 with any questions.



# Grappling with crime

- October 23 – Servers were brought back online after being restored. Contacted FBI and Oakland County Sheriff
- October 30 – Spoke to FBI on the phone, indicated there was post on the No Escape Tor site with Orion Township Public Library information
- November 10 – Someone commented on a community Facebook post that they saw the posting on the NoEscape Tor site. Forwarded information to the FBI



# First contact with patron

November 10 - Patron responded to post on community page.

Informed patron we were already working with law enforcement.

The screenshot shows a Facebook post from the Orion Township Public Library. The post text reads: "Designed to serve a population of 30,000 and house a collection of 100,000 volumes with a capacity for a 200,000 items per year circulation, the new Orion Township Public Library was spacious and inviting, offering quiet study areas, comfortable seating, meeting rooms for community gatherings, and the latest titles, as well as state-of-the-art computers and other new technologies. The company network was successfully encrypted and compromised. We have more then 220GB confidential and sensitive data, such as: Student cards with their personal data! Orders, invoice, payments, report, backup data, accounting, databases, finance, audit, billing, and thousands of other critical and confidential data. We advise you not to bring the situation to a critical level and contact us soon is possible. Assign a peson to the position of negotiator, and tell him to contact us, we will explain evrithing and help you solve this problem. Time is running out." The post includes a "Like" button and a "Send in Messenger" option. On the right side of the post, there is a red "DELETE POST AND DATA" button, a "TOTAL DATA: 220 GB" indicator, and a "NEXT UPDATE: 5D 20H 44M 00S" timer. A comment on the right side of the post reads: "Please see this claim by the threat actor stating they have obtained 220GB of sensitive data which (potentially) conflicts with your statement that no data was compromised." Below the comment is another redacted section with the text: "We have more then 220GB confidential and sensitive data, such as: Student cards with their personal data! Orders, invoice, payments, report, backup data, accounting, databases, finance, audit, billing, and thousands of other critical and confidential data."



# Round Two

- November 18 – Library web server brought down by a DDoS attack
- November 19 – We learned that the Threat Actors had posted files taken from the servers on the No Escape site

The screenshot shows a web browser window with the address bar containing the URL: <http://noescapemsqxvzdxyl7f7rmg5cdjwp33pg2wpmiaaiblb4btwtzttad.onion/post/9a7a6fee-4b30-4e30>. The browser title is "NoEscape".

The main content area displays a message:

Last Warning!!!  
We advise you not to bring the situation to a critical level and contact us soon is possible.  
Assign a person to the position of negotiator, and tell him to contact us, we will explain everything and help you solve this problem.  
Time is running out.

Below the message is a file directory listing. The files include:

- CloudLibrary - moved
- Database stats
- Envisionware Stats
- HorizonReports
- HorizonStats
- Innovative Day Rochester
- INNReach problems
- IUG 2020
- Jeff's retirement party
- Jeff's retirement party B
- McL.Cat logo
- McL.CatBackup old files
- Miscellaneous
- MUG
- New folder
- OverDrive Advantage Marc
- OverDrive Big Read
- Patron Reference
- Polaris hosted reports
- Polaris Tables 5.0
- Polaris41r2
- Strategic Plan
- tempOneNote
- Why were these in recycle Bin 021016

Other visible elements include a "NEWCO" button, a "Library" logo, and various application forms like "APPLICATION FOR BORROWER'S CARD" and "NLM Traveling Exhibitions".



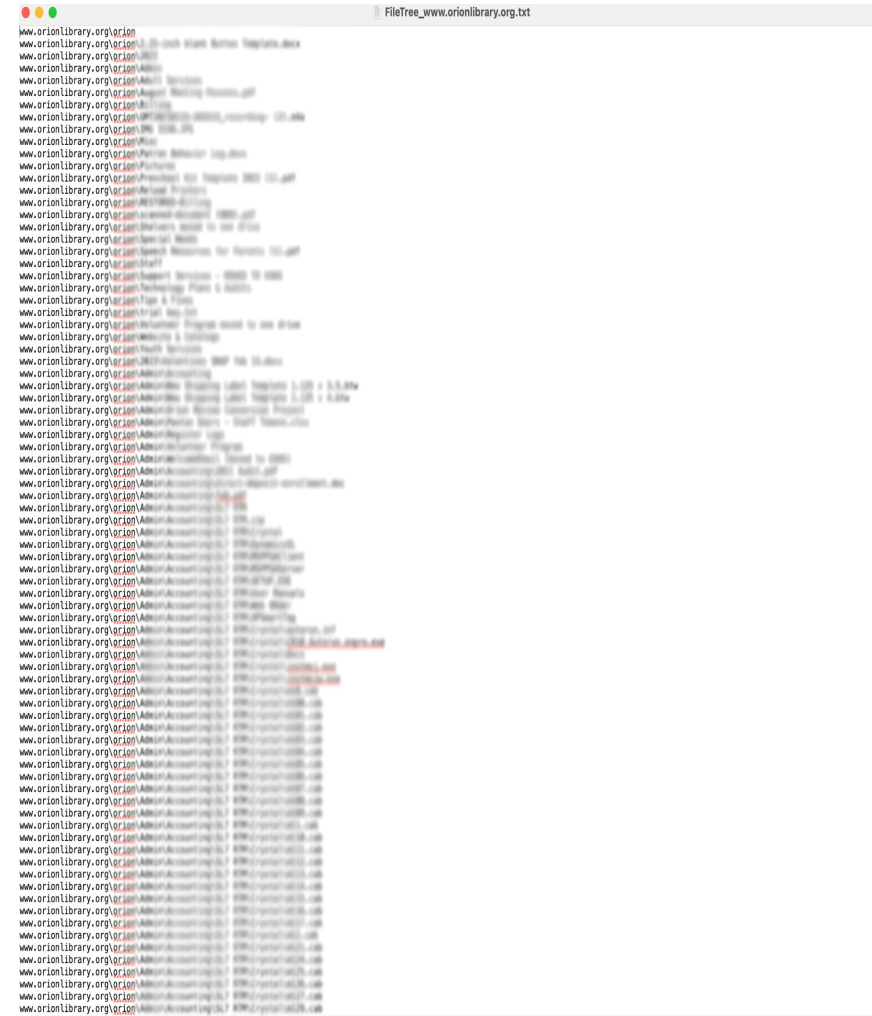
# Round Two (continued)

Became aware that there was a potential leak of information

Primary focus became assessing what information was taken and what to do about it.

Called attorney

Called insurance - now we are in business



# The Nesting Doll Approach



# Crisis Communication

11/21/23 -  
Announcement of  
ongoing cyber security  
breach.

Ran every  
communication by legal  
team.

## Library Cyberattack

It has become clear that we have been experiencing an ongoing cyberattack. The attack has affected several services, including the internet outage over the past weekend and our current website outage.

While we continue to work with law enforcement and are reaching out to third-party cybersecurity firms, we currently do not have a timeline as to when some of these services will be restored nor do we know if we may experience further outages.

We will continue to update you on this evolving situation, and we will let you know if there is any recommended action you should take.

We apologize for any inconvenience.



# Process

- Staff reviewed all files listed in the file tree to identify PII
- Counsel should supply a list of what constitutes PII - Generally things like SSN, DL numbers, DOB, signatures
- Supplied names of those potentially impacted and what information was included
- Counsel reviewed and sent notice to those that were affected
- Credit monitoring service was offered





# Meanwhile

Forensic cybersecurity experts

- Conducted an analysis of our servers

- Monitored the NoEscape Tor site

- Wrote final report of incident

- Would have negotiated with Threat Actor if we had desired

Library worked to move our website to a cloud host due to a continued DDOS attack



# Do This Now

Security - Update; Review Network Accessibility; Consider 3rd Party Penetration Testing

Consider Cloud hosting if you can afford it

Data Retention Audit - Establish regular deaccessioning of documents and **Do Not** store unnecessary PII

Insurance - Make sure your policy includes Cybersecurity coverage

Communication - Write a communication/PR policy; Craft a Crisis Communication Plan



# If You Are Hacked

**You are not facing a technical problem, you are experiencing a potential legal issue involving Personally Identifiable Information (PII)**

Shut it down

First Call - Law Enforcement

Second Call - Insurance Company

Technical Remediation

Messaging



# Helpful Resources

## Online

FBI Internet Crime Complaint Center (IC3) - <https://www.ic3.gov/>

[FCC Schools and Libraries Cybersecurity Pilot Program](#)

Library of Michigan - [Record Retention and Disposal Schedule](#)

MLA Crisis Communication Plan - <https://www.mibraries.org/intellectual-freedom-toolkit-resources>

Example Public Relations Policy - [OTPL PR Policy](#)

[MI Identify Theft Protection Act](#)

Multi-State Information Sharing and Analysis Center - <https://www.cisecurity.org/ms-isac>

[US Cybersecurity and Infrastructure Security Agency](#)

## Software

CrowdStrike / SentinelOne - industry standard security software

KnowBe4 - Security awareness training



**Questions?**  
**(ask your attorney)**



**Orion Township  
Public Library**