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

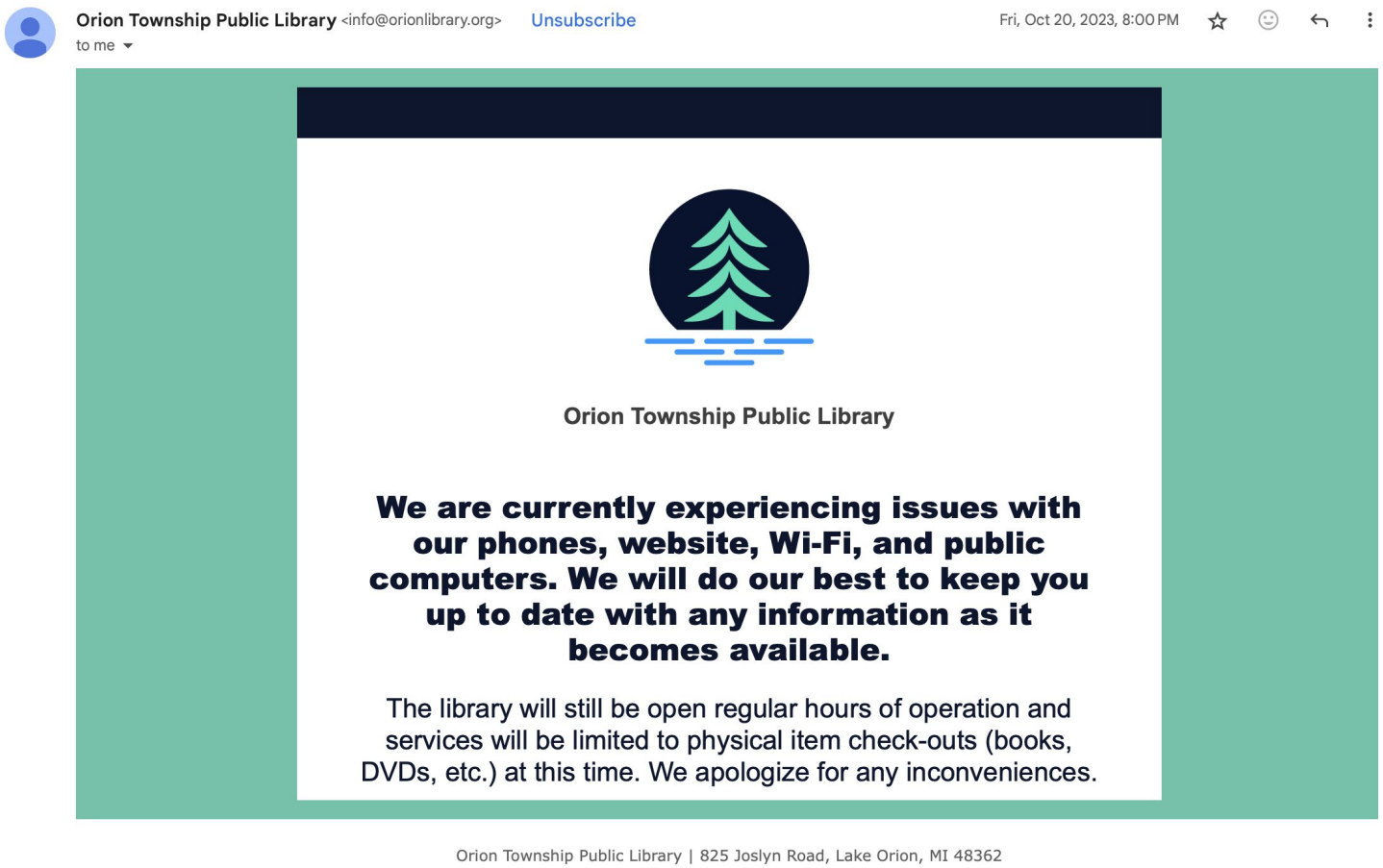
1. A small collection of documents were reported inaccessible
2. A rogue script found actively running on a virtual server
3. The host server was rebooted by staff to stop any active processes
4. IT Consultant was contacted
5. External network communication severed by staff
6. Initial assessment and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

The Villains Revealed!

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*)

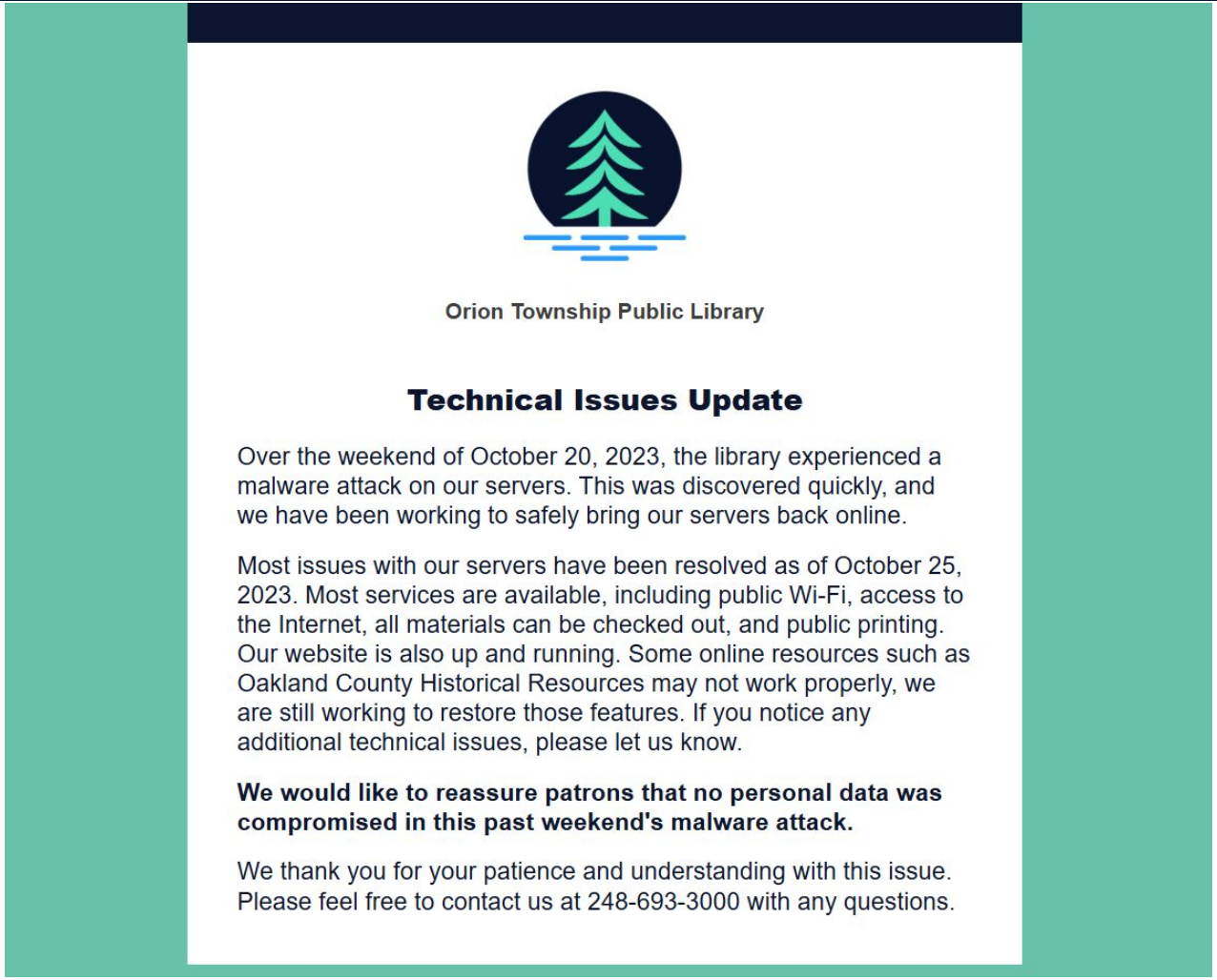
- Staff / Public Workstations and ILS unaffected
- Backups were recoverable

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.

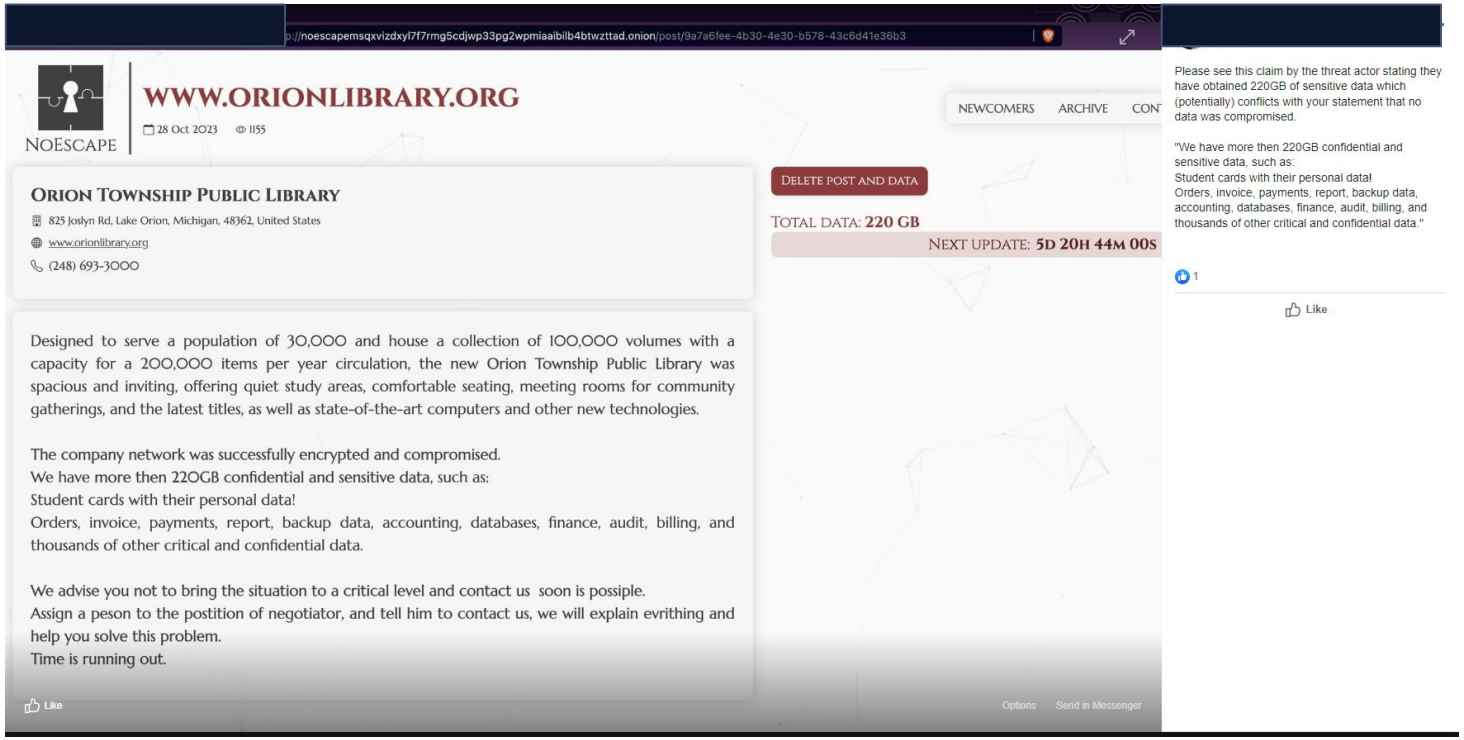
Grappling with crime

- 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

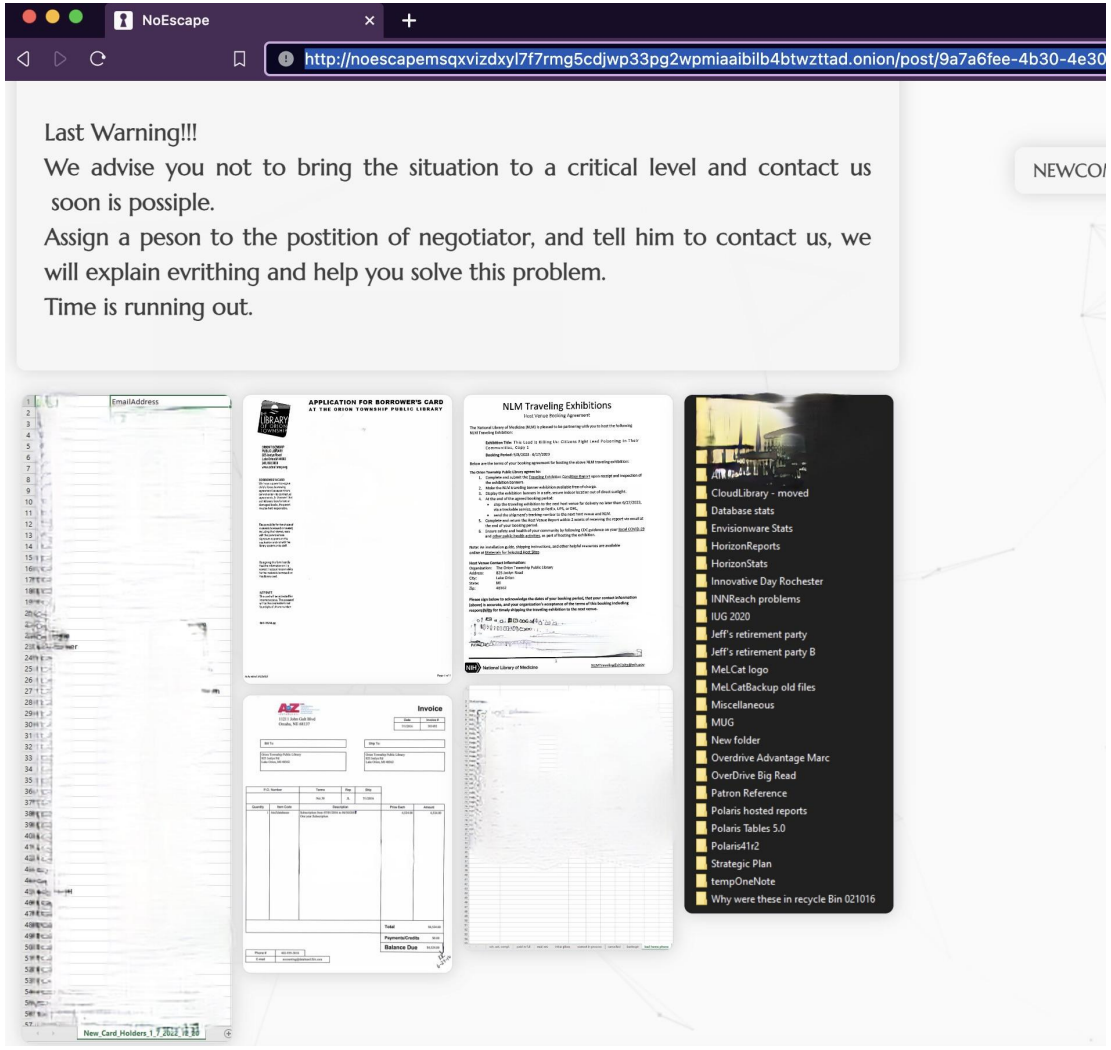
November 10 - Patron responded to post on community page.

Informed patron we were already working with law enforcement.



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



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

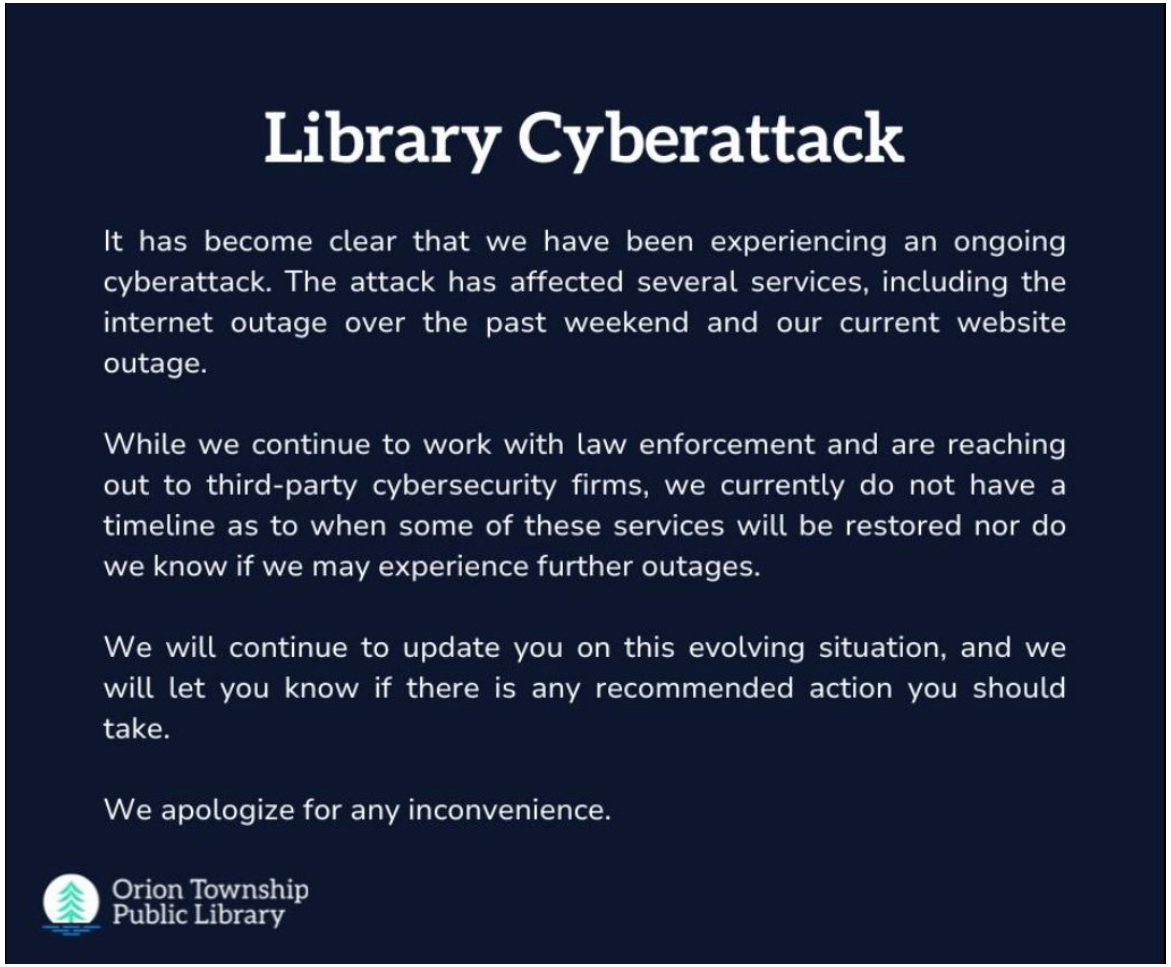
Called insurance - now we are in business

The Nesting Doll Approach

Crisis Communication

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

Ran every communication by legal team.



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.milibraries.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