

CYBER THREAT ENVIRONMENT – HEALTH & PUBLIC HEALTH SECTOR

New Hampshire Information & Analysis Center

Hannah Popovitch & Adam Ciardelli

Intelligence Analysts

Brief Classification – Warning Statement

*Handling Notice: This product contains **UNCLASSIFIED// FOR OFFICIAL USE ONLY** information. It contains information that is NOT for public release or secondary dissemination without permission from the NHIAC. Precautions should be taken to ensure this information is stored and/or destroyed in a manner that precludes unauthorized access. For questions or additional information, contact the NHIAC at NH.IAC@dos.nh.gov or (603) 223-3859.*

Health & Public Health Sector in the News

- University of Vermont Medical Center suffers a ransomware attack
- U.S. hospital victim of ransomware now defending itself in court over a babies death during the attack
- Top ransomware gangs targeting U.S. healthcare sector
 - *Includes Conti, REvil, Hive, Pysa, Clop, Ryuk*
- Microsoft BlueKeep Exploit
- More than two-thirds of healthcare CISOs surveyed reported their organizations experienced some form of data security incident within the last 12 months
 - *60 CISOs who took part in the survey reported their entities experienced phishing or business email compromise (BEC)*
- Mental healthcare providers report data breaches
 - *Two American mental healthcare provider reported data breaches that may have exposed individual's personal health information (PHI)*
 - *Did report data exfiltration from a specific period of time in March*

Health & Public Health Sector as a Target

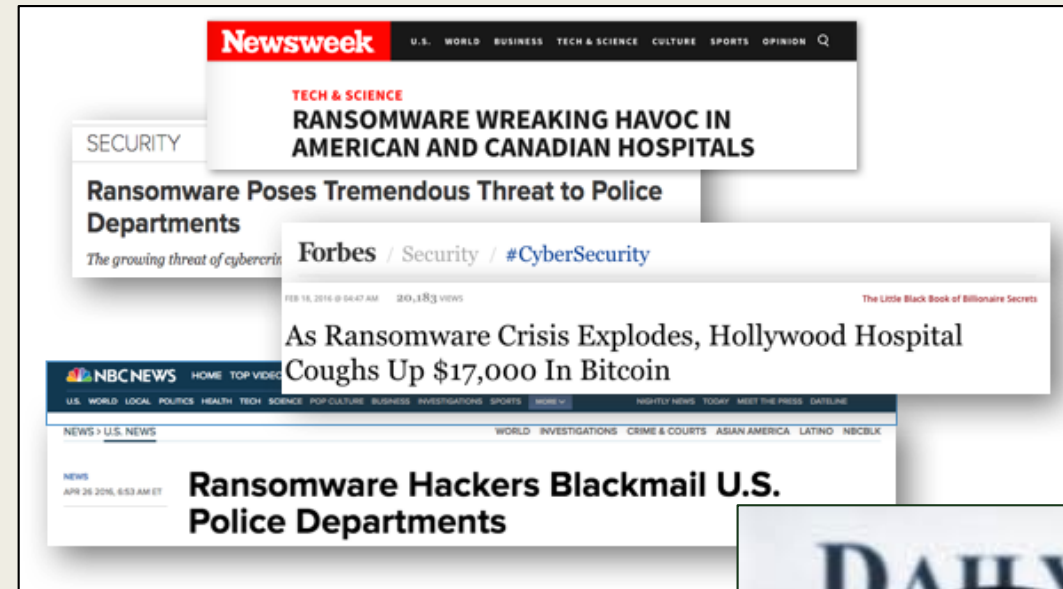
Technology is involved in the construction, operation, and maintenance of critical infrastructure.

- Personal Health Information (PHI) and Personal Identifiable Information (PII) is worth A LOT of money to attackers
- Medical devices = easy entry point for attackers
- Staff may need to access data remotely
- Staff may not be fully educated on online risks
- Large number of devices in a healthcare
- Outdated technology
- Ability to transverse a network
- Greater likelihood to pay

Critical to our EVERYDAY lives.

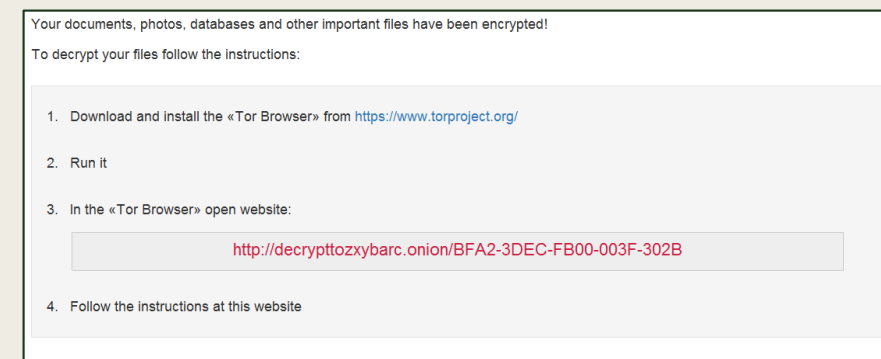
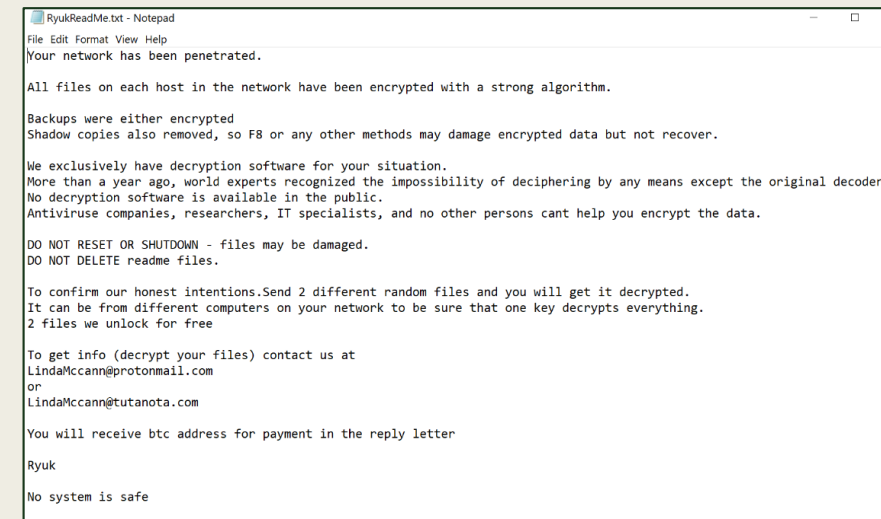
Cyber Threats

- Ransomware
- Phishing Emails
- Denial of Service
 - *Distributed Denial of Service (DDoS)*
 - *Telephony Denial of Service (TDoS)*
- Data Breaches
- Improper Usage & Internal Attacks
- Misinformation & Disinformation



Ransomware

- A type of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable and will display messages demanding a fee to be paid in order for your system to work again
- Demands can range from the thousands to the millions – paid in a form of cryptocurrency, generally Bitcoin
- Average Downtime = Approximately 23 Days
- Cost in Disruption to Services 5-10x higher than the ransom
- Exfiltration of Data
 - *Exfiltration: Data exfiltration occurs when malware and/or a malicious actor carries out an unauthorized data transfer from a computer.*
 - *81% of ransomware attacks involved the threat to leak exfiltrated data*
 - *Second ransom demand for the potential to post exfiltrated data to the internet*



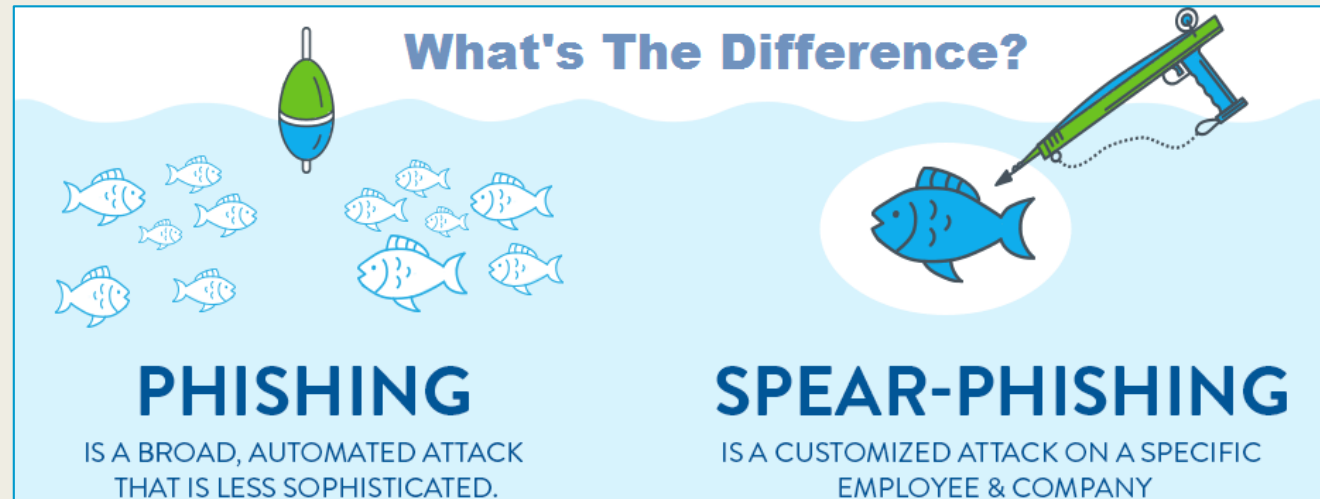
UVM Medical Center

- Malware on more than 5,000 hospital computers and laptops; encrypted files and data on 1,300 servers
- Had to wipe the computers, laptops, and servers
 - *Then reinstall all data and software*
- Furloughed or reassigned about 300 employees who were unable to perform their jobs
- UVM Medical Center and affiliated locations canceled or postponed some services, including elective procedures and cancer treatments
- This one attack cost UVM Medical Center around \$1.5 million per day in lost revenue and expenses to restore its computer systems

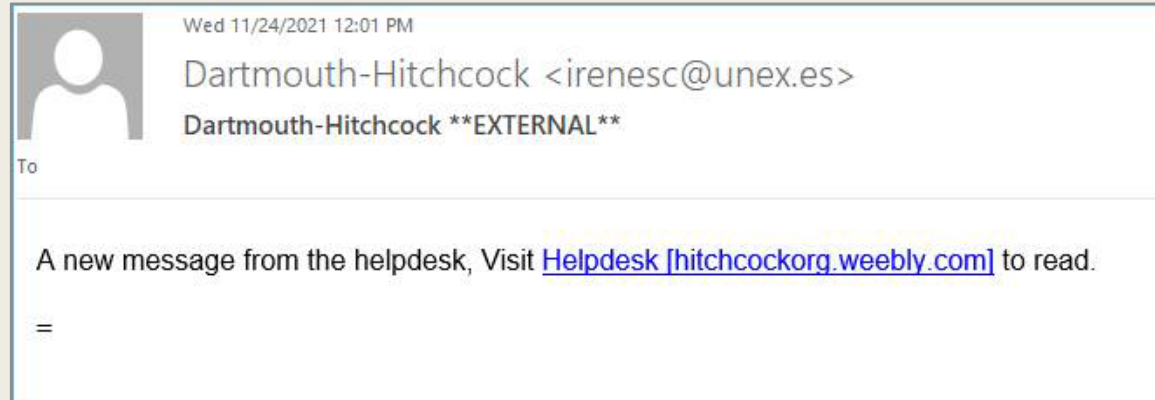
Phishing

- **Phishing** is a fraudulent attempt to obtain sensitive information by disguising oneself as a trustworthy entity in an electronic communication
- **Spear phishing** is an attack on a targeted individual, organization, or business
- Often looking to obtain usernames, passwords, credit card information, Person Identifiable Information (PII), Protected Health Information (PHI), access to sensitive information/databases
- Phishing emails often contain malicious links or malicious attachments

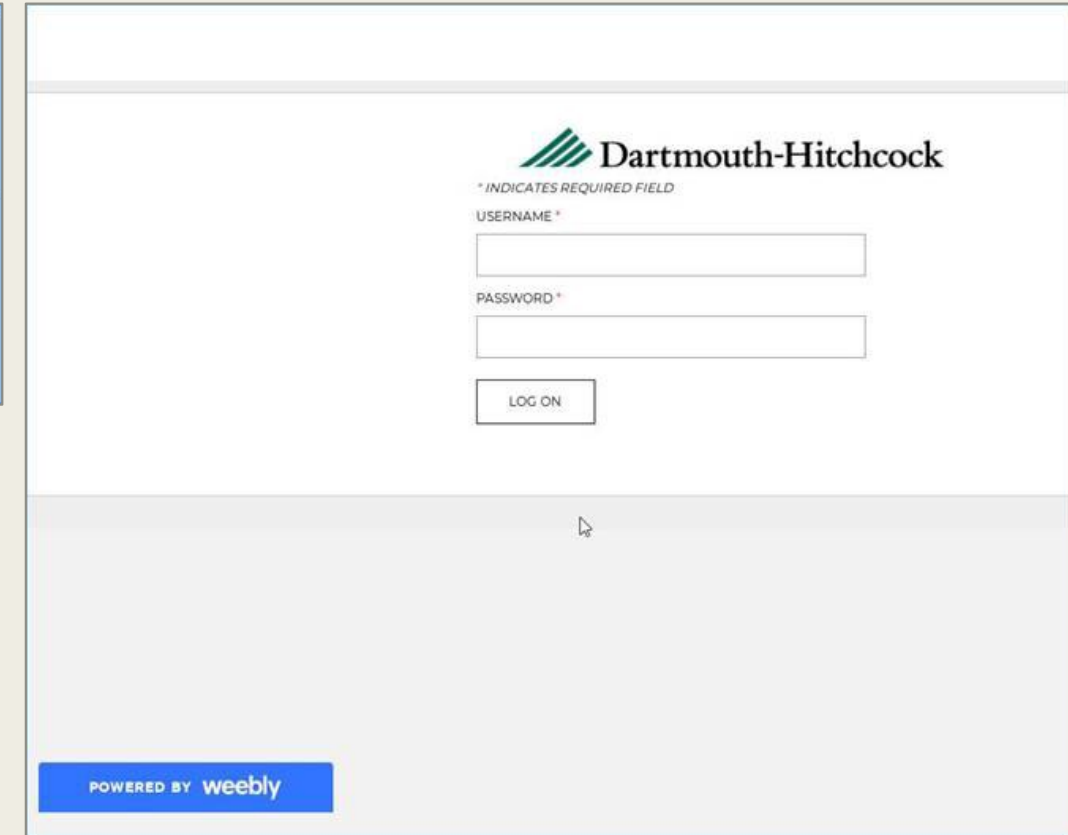
THE USER IS THE FIRST AND LAST LINE OF DEFENSE AGAINST PHISHING EMAILS!



Highly Targeted Phishing Email

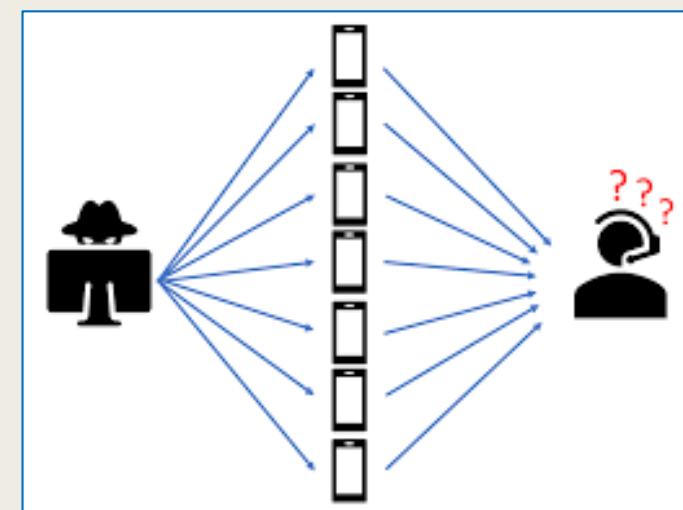
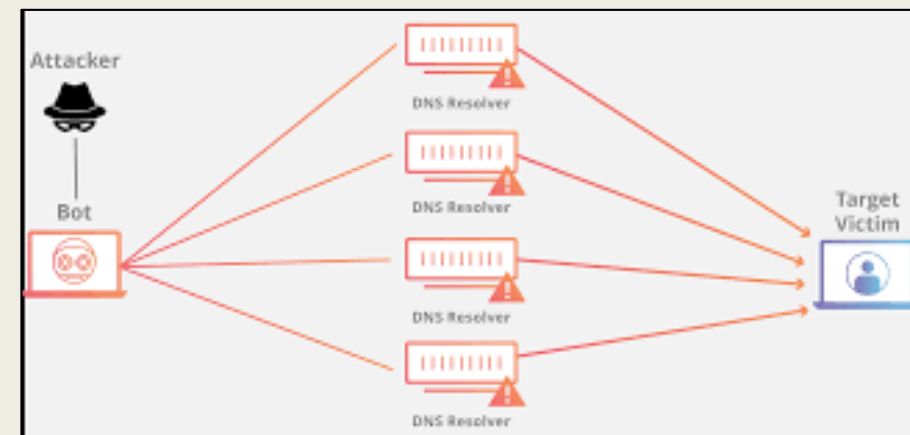


- Demonstration of a calculated, coordinated effort to attack a New Hampshire health system
- Imperative to invest in an industry-leading enterprise email fraud defense solution, and properly operationalize that solution with talented staff
- Enterprise-wide access to commodity web hosting platforms including, but not limited to, Weebly should be heavily scrutinized
- In line with previously distributed guidance in federal cybersecurity information products, holidays are a moment of opportunity for threat actors



Denial of Service: Distributed Denial of Service (DDoS) & Telephony Denial of Service (TDoS)

- DDoS: An attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet
 - *Each bot sends a request to the victim IP repeatedly causing the server or network to become overwhelmed*
 - *Causing the server or network to crash*
- Controlled through bots or botnets
- TDoS: An attempt to make a telephone system unavailable to the intended user by preventing incoming and/or outgoing calls
 - *Done by calling the system repeatedly to overwhelm it*



New Hampshire TDoS Examples

- New Hampshire Hospital victim of TDoS attack – 80% of their phone lines were completely tied up
- No calls could go in or out for approximately 20 minutes
- This included calls from within the hospital – one department could not call another
- Calls appeared to be coming from New York



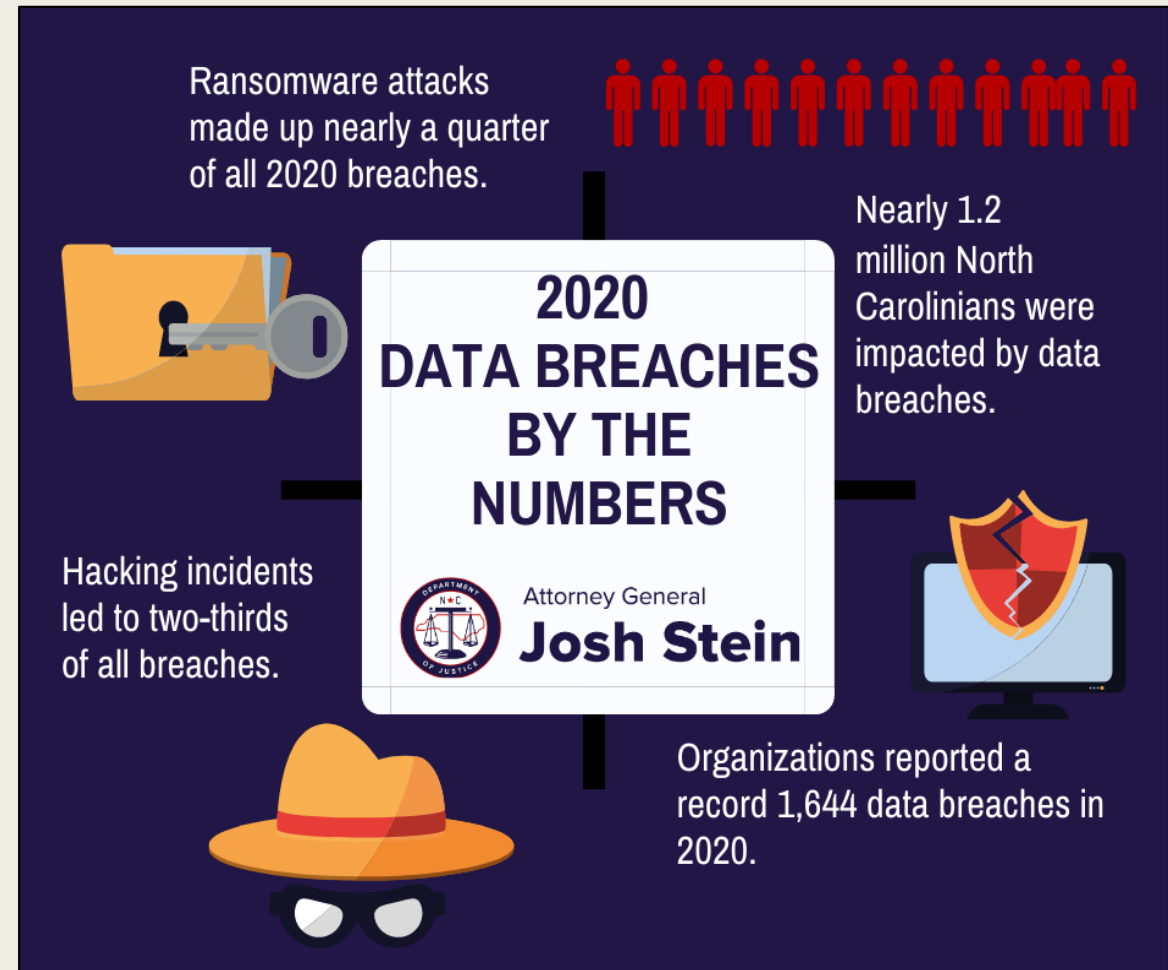
- Unintentional TDoS attack on hospital due to COVID-19 measures
- Initiated by a group who was upset with how the hospital was handling COVID-19 patients
- Received, at minimum, 550 calls regarding this

**TDoS attacks could
cost lives, warns FBI**

**TDoS Attacks Take
Aim at Emergency
First-Responder Services**

Data Breach

- Intentional or unintentional release of secure, private or confidential information to an untrusted environment
- Could be looking for...
 - *Sensitive information*
 - *Personally Identifiable Information (PII)*
 - *Company information*
- 68% of breaches take months or longer to discover
 - *Looking at network topology*
 - *Exfiltrating data*



Improper Use & Internal Attacks

- Employees, collectively, have access to the entire system
- Insider threat
 - *Most impactful threat to organization*
 - *Often falls under the radar*
 - *Isn't just IT who could be working to do this*
- Undergo training but human error or irresponsible employees can complicate things
 - *Move to working remote, freedom to log in from a variety of devices and transfer data between networks*
 - *Employees with access to large amounts of information*

Three categories of insider threats



Compromised

Threat actors who have stolen a legitimate employee's credentials pose as authorized users, utilizing their accounts to exfiltrate sensitive data. Employees often don't know they have been compromised.



Negligent

Employees without the proper security awareness training can inadvertently misuse or expose confidential data, often as a result of social engineering, lost/stolen devices or incorrectly sent emails/files.



Malicious

Bad actors—such as current or former employees, third parties or partners—use their privileged access to steal intellectual property or company data for fraud, sabotage, espionage, revenge or blackmail.

Insider Threat - Texas

- Insider victimized a Texas hospital while using the hospital network to attack rival hacking groups
- Caught after filming himself “infiltrating” the hospital network
 - *Used a specific key to “infiltrate” the system, revealing his identity*
- Downloaded malware on dozens of machines – including nursing stations with patient records
- Built a backdoor in the HVAC system – if the HVAC system fails it would cause damage to drugs and medicines
- Individual plead guilty to computer tampering, serving a 9 year sentence in addition to paying \$31,000 in fines

Misinformation, Disinformation, Malinformation (MDM)

- **Misinformation** is false, but not created or shared with the intention of causing harm.
- **Disinformation** is deliberately created to mislead, harm, or manipulate a person, social group, organization, or country.
- **Malinformation** is based on fact, but used out of context to mislead, harm, or manipulate.
 - *Information Activities When Released by Foreign Actors = **Foreign Influence***



MDM → Physical Threat

- **Some Domestic Violent Extremists (DVE) Motivated by conspiracy theories**
 - DVEs motivated by conspiracies will likely threaten violence or plot against healthcare personnel, facilities, and public officials in response to COVID-19 mitigation measures
-
- * Sep 2021, 3x incidents at CA hospital, individual claiming “COVID is fake, vaccines cause death”, threatened to shoot healthcare workers,
 - * May 2021, extremist incited violence against vaccinations sites on social media channel
 - * Jan 2021, chief medical advisor to the president received death threats relating to COVID response
 - * Mar 2020, spread of MDM online led to attempted train derailment attack against US Navy hospital ship providing COVID relief in the Port of Los Angeles



COVID-19 Disinformation Toolkit

- Toolkit with resources to help State, local, tribal and territorial (SLTT) officials bring awareness to MDM, and conspiracy theories appearing online related to COVID-19's origin, scale, government response, prevention and treatment.
- Designed to be tailored with local government websites and logos.
- <https://www.cisa.gov/covid-19-disinformation-toolkit>



Additional Disinformation Tools

RAND Corporation database of web tools.

Identifies and collects in one place a set of resources that can help users combat the challenge of disinformation.

- <https://www.rand.org/research/projects/truth-decay/fighting-disinformation.html>
- <https://www.rand.org/research/projects/truth-decay.html>
- NHIAC can share links upon request!

Countering Truth Decay

A RAND Initiative to Restore the Role of Facts and Analysis in Public Life



Photo by vepar5/Adobe Stock

Tools That Fight Disinformation Online

Search for tools that fight disinformation by name, type, or by keyword:

fact-checking

SEARCH

examples: Hamilton 2.0, bot detection, fact-checking

HIDE ALL TOOL CATEGORIES ^

Bot/spam detection

Education/training

Codes and standards

Verification

Credibility scoring

Whitelisting

Disinformation tracking

20 results | [Clear all filters](#)

What can you do?

Mitigation Strategies

- Start an open conversation surrounding potential cyber attacks with ALL employees
- Encourage questions – no question is a bad question
- Ensure that all employees know who to contact when/if they receive a malicious or suspicious file, attachment, link, or email
- Have IT communicate with employees about trends and best practices more often than just employee orientation
- Encourage good cyber hygiene – changing your password every 90 days, using a mix of symbols, letters, and numbers, making your password 12 characters or longer (passphrase)

Time it takes a Hacker to Brute Force your password

@coders.bro

Numbers of Character	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	1 sec	5 secs
7	Instantly	Instantly	25 secs	1 min	6 mins
8	Instantly	5 Secs	22 mins	1 hour	8 hours
9	Instantly	2 mins	19 hours	3 days	3 weeks
10	Instantly	58 mins	1 month	7 months	5 years
11	2 secs	1 day	5 years	41 years	400 years
12	25 secs	3 weeks	300 years	2k years	34k years
13	4 mins	1 year	16k years	100k years	2m years
14	41 mins	51 years	800k years	9m years	200m years
15	6 hours	1k years	43m years	600m years	15bn years
16	2 days	34k years	2bn years	37bn years	1tn years
17	4 weeks	800k years	100bn years	2tn years	93tn years
18	9 months	23m years	6tn years	100tn years	7qd years

Are you in green zone?

Cyber Tips

- Misspelled words and incorrect grammar are a hint for a malicious email
- Pay attention to the sender's address and verify that it is indeed from a trusted sender
- If it contains an offer that sounds too good to be true, it most likely is! Delete it.
- Verify links and attachments BEFORE opening them
- An email requiring personal information is often suspect. Be sure to reach out to the email sender by phone, prior to providing any personal information including usernames, passwords, social security information, or credit card information.
- Emails that seem out of the ordinary should be verified
- Report any unusual computer activity (such as the IOCs) to your IT Department

Reporting Cyber Attacks

- Report to your organization's IT department
- Intelligence and information sharing with ALL stakeholders
- Without reporting, unable to provide assistance/intelligence, and fully understand the threat environment in New Hampshire
- NHIAC & NHCIC Cyber Reporting Portal
- Report a cyber-incident whenever...
 - *the confidentiality,*
 - *integrity, and/or*
 - *availability of your organizations systems is potentially compromised*

www.nh.gov/safety/cyber



Thank you!

Hannah Popovitch

Intelligence Analyst

Direct: (603) 223-3740

Fax: (603) 271-0303

Email: Hannah.L.Popovitch@dos.nh.gov

Adam Ciardelli

Intelligence Analyst

Direct: (603) 223-8985

Fax: (603) 271-0303

Email: Adam.J.Ciardelli@dos.nh.gov

New Hampshire Information & Analysis Center

Direct: (603) 223-3859

Tip Line: (603) 3860

Fax: (603) 271-0303

Email: NH.IAC@dos.nh.gov