



# Information Security Awareness Training

This course will discuss measures to protect you and Crouse from information and security breaches.



# Weak Passwords

- Contain less than 8 characters
- Password is a word that can be found in a dictionary
- Uses Common words such as:
  - Names of family members
  - Names of pets
  - Names of Co-workers
  - Names of characters from shows
- Uses other common words such as:
  - Computer names
  - Computer terms
  - Computer commands
  - Website names
  - Company names
  - Hardware names
  - Software names

## Examples of Bad Passwords:

- CrouseHospital
- Syracuse
- sanjose
- billyjoe
- Fluffy
- Windows
- Etc.

## Other features of weak passwords Include:

- Birthdays
- Addresses
- Phone numbers

## Word or number Patterns:

- Aaabbbb
- Qwerty
- 123321



# Strong Passwords

Strong Passwords contain AT

LEAST 3 of the 5

Characteristics:

- Lowercase Letters
- Uppercase Letter
- Numbers
- Punctuation (e.g. ?! Etc.)
- Special Characters (e.g. @ # \$ % ^ & \* () + etc.)
- Contain at least 8 Characters
- The longer and more complex the password, the harder it is to crack

Passwords Should be easy to remember, but also complex and hard to guess.

Creating a phrase or mixing a string of words, such as a color, animal, activity, number, punctuation, and special character.

For example:  
7blueZebrasDance!



# Additional Password Notes

## Password Protection Standards:

- Never use your Crouse Hospital password outside of Crouse (personal email, bank account etc.) If one password were to be cracked all passwords would be compromised.
- Do Not share your Crouse username or Password with anyone (Not even IT) Password must be treated as sensitive and confidential.
- Do Not Write down your password or store your password on-line without encryption.
- Do Not speak about the password in front of others.
- Do Not hint at the format of the password (e.g. my family name)
- Do Not reveal password on questionnaires or security forms.
- If Someone demands a password, refer them to Crouse's Information Security Team.
- Always decline the use of "remember password" feature of applications when possible.

If an account or password compromise is suspected, please report the incident to the Information Security Team.

Any Employee found to have Violated Crouse's Policy on passwords may be subject to disciplinary actions up to and including termination of employment.



# Multifactor Authentication (MFA)

- Multifactor Authentication or MFA is another means of verifying that it is you who is signing into an application, online account, or Remote gateway session.
- When you enter your username and password into specific applications it will send you a text code or a push to your phone that must be approved to sign in.
- MFA is currently required for Email for first-time registration and access outside the Crouse network and RDP



# Social Engineering

- The use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes.
- Social Engineering is used for financial gain by extorting confidential information and selling the information or Ransoming the information.
- Social Engineering Can be done via Email (Phishing), Phone Calls (Vishing) Text Messaging (Smishing) and even in person where they impersonate employees, delivery workers or others to be granted access to restricted areas.

## Social engineering Statistics

- 98% of Cyber Attacks Involve Some Form of Social Engineering
- 61% of breaches happen because of employee negligence.
- 90% of cyberattacks target an organization's employees.



# Phishing

- Is an attempt to get confidential information by pretending to be a trustworthy entity in an electronic communication (ex. Co-worker, friend, company etc.)
- Phishing emails will try to elicit an emotional response from you.
- Kindness, Sadness, Curiosity, Greed, Fear etc. These emotions are Key Identifiers for phishing emails
- These emails will seem authentic in nature, which makes it sometimes difficult to tell it's fake.

## Examples of Phishing include:

- Request for personal information (name, address, social security)
- Web links to suspicious websites that appear legitimate.
- Irrational requests for financial compensation (Gift Cards, Venmo, PayPal)
- Grammatical Errors
- Inconsistencies in Email Addresses, Links & Domain Names
- Suspicious Attachments



# Tailgating

- Tailgating attacks are where an attacker follows an unaware user to gain access to an area without authorization.
- Criminals may pose as someone who looks like they have appropriate credentials to access a restricted area, such as a delivery person, vendor, state employee etc.
- Example: A criminal dressed as a delivery driver carrying boxes is allowed into a restricted area without being asked for credentials or verification.





# Baiting

- Baiting is when a criminal uses something enticing to get a user to give up confidential information.

Examples:

- Criminal creates a website claiming you can download a movie, when the user goes to access the download, it infects their computer system with Malware or prompts the user to enter confidential information.
- Criminal infects a USB flash drive with malware and leaves it in a high traffic area hoping a user will pick up the drive and plug it into a computer which releases the malware into the computer system



# Quid Pro Quo

- Quid Pro Quo is when a criminal offers help to someone in need in exchange for confidential information.
- This process is used to get username/password, door access codes, or install malware/viruses.
- Quid Pro Quo means “something in exchange for something”

Example:

- A Criminal calls pretending to be IT and finds someone needing assistance. They fix the problem in exchange for confidential information or access.



# Email Hygiene

- NEVER open emails from untrusted sources.
- DO NOT Download any suspicious attachments or click on unknown suspicious website links.
- Clicking suspicious links or downloading suspicious attachments can lead to virus infecting and disrupting Network systems as well as Electronic Medical Record systems.
- Always check email addresses, body of text and personal signatures to determine if the source is who they claim to be.
- Report any and All suspicious emails using the Report Phish Button in the upper right-hand corner of your Outlook client. Or Contact [spam@crouse.org](mailto:spam@crouse.org)



# Malware

- Malware refers to any software designed to have a malicious purpose once deployed to a computer or network. Malware infection typically occurs without a user's knowledge, often because it camouflages itself as a different file type such as an image or PDF file.

## Methods Of Infection:

- Phishing
- USB
- Websites
- Infected Files



# Ransomware

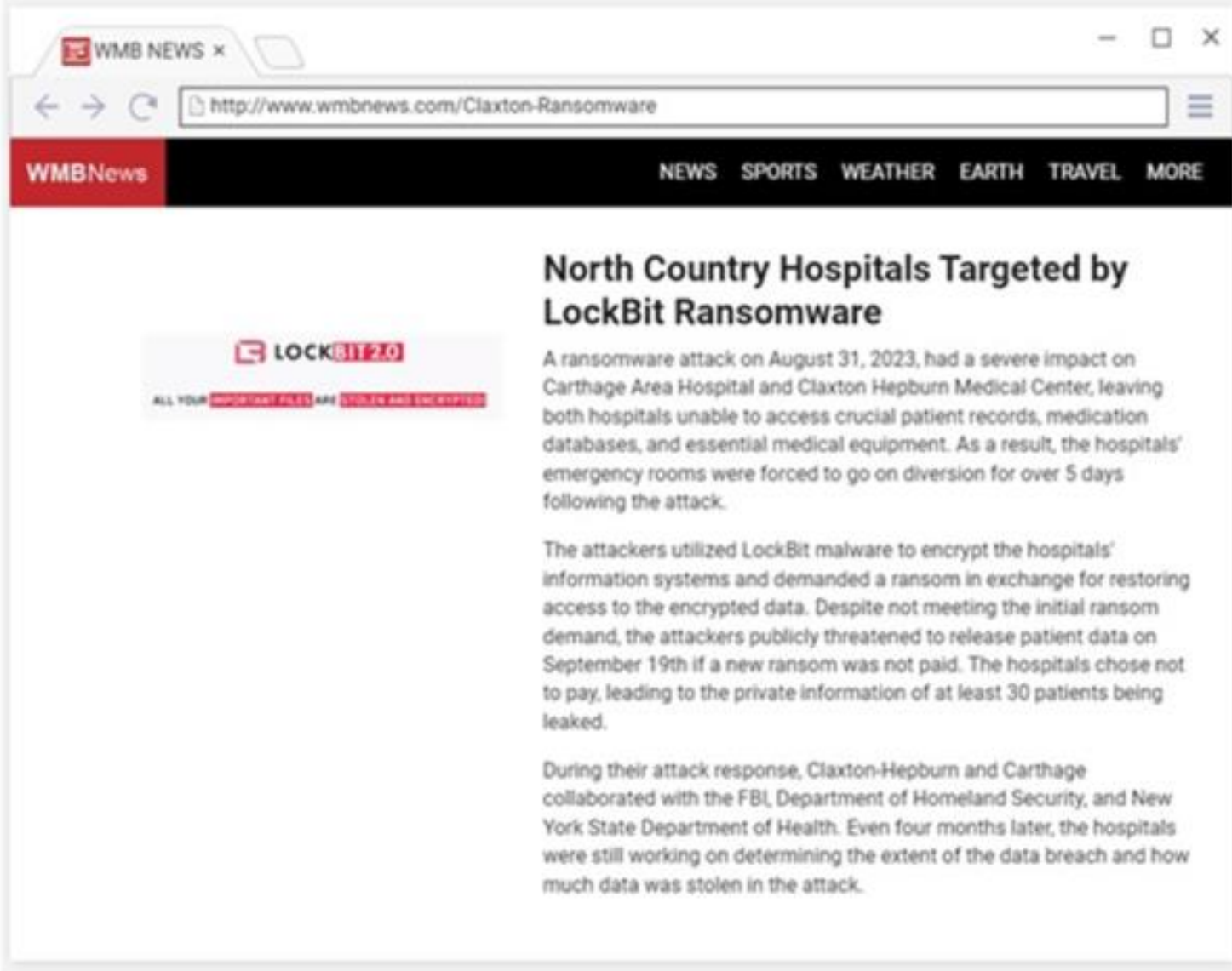
- Ransomware is a malicious software or Malware that encrypts files within a network system and holds important data/files at ransom. An Organization's critical data is encrypted so that they cannot access files, databases, or applications.
- Ransomware is typically deployed using some form of social engineering, like phishing.
- Ransomware will cripple an organization if it is introduced to the network system. It is everyone's role to protect Crouse from Ransomware attacks.

What do you do if you encounter Ransomware at Crouse?

- Step 1: Don't Panic!
- Step 2: Unplug the Network Cable/Disconnect Wi-Fi
- Step 3: Report the information to the



## Real Attacks: Claxton



The screenshot shows a web browser window with the address bar displaying <http://www.wmbnews.com/Claxton-Ransomware>. The page header includes the WMBNews logo and navigation links for NEWS, SPORTS, WEATHER, EARTH, TRAVEL, and MORE. The main article is titled "North Country Hospitals Targeted by LockBit Ransomware". To the left of the text is a graphic with the LockBit ransomware logo and the text "ALL YOUR IMPORTANT FILES ARE LOCKED AND CRYPTED". The article text describes a ransomware attack on August 31, 2023, at Carthage Area Hospital and Claxton Hepburn Medical Center, detailing the impact on patient records and emergency services, and the subsequent ransom demand and data breach.

### North Country Hospitals Targeted by LockBit Ransomware

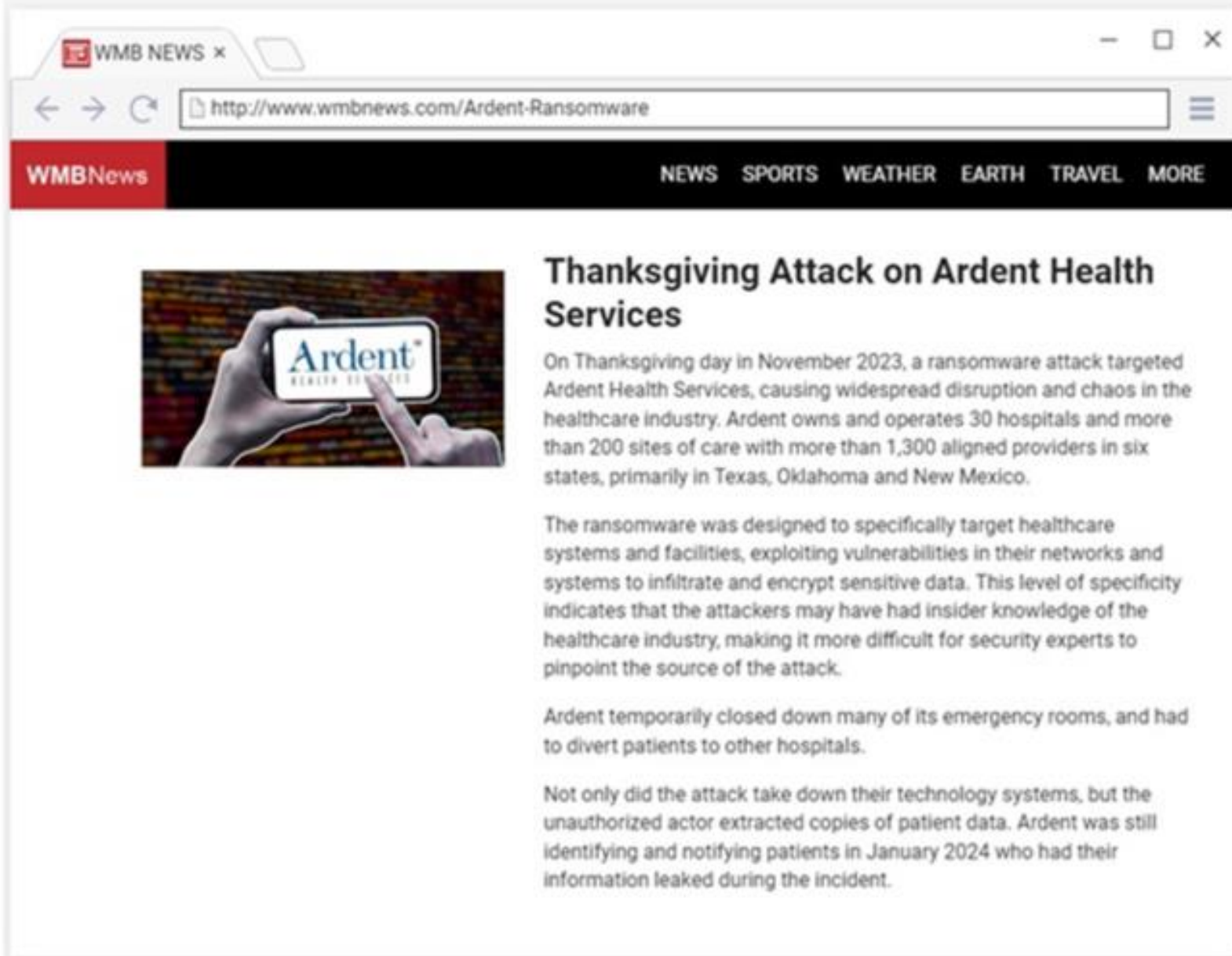
A ransomware attack on August 31, 2023, had a severe impact on Carthage Area Hospital and Claxton Hepburn Medical Center, leaving both hospitals unable to access crucial patient records, medication databases, and essential medical equipment. As a result, the hospitals' emergency rooms were forced to go on diversion for over 5 days following the attack.

The attackers utilized LockBit malware to encrypt the hospitals' information systems and demanded a ransom in exchange for restoring access to the encrypted data. Despite not meeting the initial ransom demand, the attackers publicly threatened to release patient data on September 19th if a new ransom was not paid. The hospitals chose not to pay, leading to the private information of at least 30 patients being leaked.

During their attack response, Claxton-Hepburn and Carthage collaborated with the FBI, Department of Homeland Security, and New York State Department of Health. Even four months later, the hospitals were still working on determining the extent of the data breach and how much data was stolen in the attack.



## Real Attacks: Ardent




The image shows a browser window with the URL <http://www.wmbnews.com/Ardent-Ransomware>. The page features a navigation bar with "WMBNews" and links for "NEWS", "SPORTS", "WEATHER", "EARTH", "TRAVEL", and "MORE". The main content includes a photograph of a hand holding a smartphone displaying the Ardent Health Services logo, a headline "Thanksgiving Attack on Ardent Health Services", and three paragraphs of text detailing the ransomware attack on Thanksgiving day in November 2023, the specific targeting of healthcare systems, and the impact on emergency rooms and patient data.

WMB NEWS x

← → ↻ <http://www.wmbnews.com/Ardent-Ransomware>

WMBNews NEWS SPORTS WEATHER EARTH TRAVEL MORE



### Thanksgiving Attack on Ardent Health Services

On Thanksgiving day in November 2023, a ransomware attack targeted Ardent Health Services, causing widespread disruption and chaos in the healthcare industry. Ardent owns and operates 30 hospitals and more than 200 sites of care with more than 1,300 aligned providers in six states, primarily in Texas, Oklahoma and New Mexico.

The ransomware was designed to specifically target healthcare systems and facilities, exploiting vulnerabilities in their networks and systems to infiltrate and encrypt sensitive data. This level of specificity indicates that the attackers may have had insider knowledge of the healthcare industry, making it more difficult for security experts to pinpoint the source of the attack.

Ardent temporarily closed down many of its emergency rooms, and had to divert patients to other hospitals.

Not only did the attack take down their technology systems, but the unauthorized actor extracted copies of patient data. Ardent was still identifying and notifying patients in January 2024 who had their information leaked during the incident.



## Real Attacks: Change



### Change Healthcare Hack Cripples Payment Systems for Health Providers

The healthcare industry continues to face challenges in recovering from a cyberattack that targeted Change Healthcare in February 2024.

The attack, carried out by the BlackCat ransomware group demanded a ransom of \$22 million. This prompted Change Healthcare to disconnect over 111 services in order to prevent further harm. The company took steps to collaborate with law enforcement and cybersecurity experts in order to mitigate the ransomware threat.

At the peak of the incident:

- Healthcare providers such as physicians and hospitals experienced disruptions in billing, prescription management, and healthcare procedures. This included Crouse!
- Pharmacies were also affected, leading to difficulties in obtaining information and accurately filling prescriptions.
- Some individuals had to pay full price for medications out of pocket due to the pharmacies losing access to coverage verification methods.





# Common Ransomware Infection Methods



Email is the Most Common Method



Free or Pirated Software



Surfing the Web



Malicious or Compromised Websites



## How Can I Tell If My Computer Is Infected?

Look for any or all of these characteristics:

- You suddenly cannot open files you could open before
- Errors appear telling you the file is corrupt, cannot be found, or it has the wrong extension
- You see a payment countdown window, program, or ransom demand instructions
- Files you didn't create or add appear on your desktop that look like ransom demand instructions

