MALICIOUS SOFTWARE INSTALLED THAT CAN ENCRYPT DATA AND FILES, BLOCK USER ACCESS, EXFILTRATE DATA AND FILES, ETC.

MALWARE
Type of malware that encrypts sensitive data and files to then demand a ransom to unlock the encrypted information.

RANSOMWARE
A form of social engineering in which cybercriminals “go fishing” for victims by sending emails, seemingly from trusted parties, with promises, opportunities, or threats to deceive victims.

PHISHING
A form of social engineering in which cybercriminals “go fishing” for victims by sending emails, seemingly from trusted parties, with promises, opportunities, or threats to deceive victims.

DENIAL OF SERVICE (DOS)
An attack that sends massive volumes of traffic to overwhelm an organization’s website or server.

WHY ARE LOCAL GOVERNMENTS TARGETED?

1. Local governments store considerable amounts of sensitive information known as personally identifiable information (PII) which includes, names, addresses, driver’s license numbers, credit card numbers, social security numbers, and medical information.

2. Cybercriminals are experts at what they do. In recent years, the availability of low-cost hacking tools has made it relatively easy to enter the cybercrime business and target local governments due to their low security and strict budgets.

3. Local governments are often viewed as enticing “soft targets” – as they tend to lack the funding and resources to defend themselves against an attack.
RECENT EVENTS

APRIL 2021
- A Greater Minnesota city was targeted by a cyberattack and it took city officials a day to even realize it was a ransomware attack. The hackers demanded a ransom of $60,000 in order to release the data back. The city agreed to pay the ransom, however the hackers demand another $120,000. This time the city refused to pay the ransom again, at the risk of losing the data. Fortunately the city was able to recover its most crucial files on an offline desktop.

JANUARY 2019
- A Minnesota county experienced a data breach after the IT department discovered unusual activity from within the county’s email system. The county quickly shut down the email system and hired forensic IT specialists. The specialists determined the breach was caused by a phishing email linked to 11 other accounts. The investigation in February 2020 and revealed that confidential information from 12,320 individuals was contained in the emails and document attachments. Since the attack, the county has taken preventative measures to enhance the security of its entire system.

OCTOBER 2019
- A Greater Minnesota county experienced a data security breach through a phishing email. The hacker accessed an employee’s email, obtaining private and confidential information. The county launched an investigation with IT forensic specialists. Which revealed that the hacker had gained access to the personal information of around 4,400 individuals. The county notified those whose data had been compromised and provided information on the incident, along with steps to take to monitor and protect their private information.

THE MODERN RANSOMWARE ATTACK LIFECYCLE

PHISHING EMAIL
MALICIOUS VIRUS IS ACTIVE
INSTALL MALWARE
OWN DOMAIN CONTROLLER
STEAL CREDENTIALS
MOVE LATERALLY
STEAL DATA
INSTALL RANSOMWARE
DEMAND RANSOM

AT A GLANCE

95% OF DATA BREACHES ARE DUE TO HUMAN ERROR

80% OF THOSE DATA BREACHES ARE DUE TO PHISHING EMAILS

EVERY MONTH
Minnesota IT services (MNIT) defends against around 27,000 phishing emails and messages targeting state employees.

EVERY 11 SECONDS
A ransomware attack is carried out globally.

HELPFUL RESOURCES
- STOPRANSOMWARE.GOV
- icma.org/topics/cybersecurity
- MN.GOV/mnit