RANSOMWARE

Hackers are using ransomware to target everyone, from consumers to businesses big and small, to municipalities, and the payoff is huge.

Plainfield, New Jersey, a town of roughly 50,000 people, fell victim to hackers and is still working to get its files back.

Mayor Adrian Mapp said hackers infiltrated their computer systems when an employee clicked on an infected link. City officials scrambled to pull servers offline, but three were compromised, leaving emails and other city files inaccessible.

"We have about 10 years of documents that we are not able to access," the mayor said.

The hijackers held the files ransom, demanding roughly 650 euros paid in bitcoin. Mapp sought the assistance from law enforcement, but remains helpless in regaining access.

Plainfield was a victim of ransomware, a type of malware that cybersecurity experts and law enforcement officials say is spreading nationwide.

"Everyone should be concerned. It's the number one problem facing the computer security industry and it's very, very difficult to solve," said Ryan Naraine, director at cybersecurity firm Kaspersky Lab. Naraine said the malware gets into people's computers, often with a simple click.

"They prey on people's willingness to click on the latest viral videos, they prey on people's willingness to click on Facebook links, they are even sending spam in addition to emails through Twitter," Naraine said.

Once a computer is infected, it encrypts all files or locks the user out until they pay for the key. Naraine demonstrated how it works.

"I have a music file and like many people, I have photos, often family photos," Naraine said. "The ransomware is communicating with a server. The server is sending instructions here to start encrypting all these files."

In just minutes, the ransomware takes hold and the computer is compromised.

"The machine is now ransomed -- this machine is now part of the ransomware attack," Naraine said. "If I try to look at all my photos from my last family vacation, you try to open, it's nothing. It's garbage. Imagine an average business -- not only on this computer but encrypting every computer within this a network at the same time."

In addition to a string of hospitals hacked, the village of Ilion, New York paid hundreds of dollars in ransom in 2014 and the police department in Melrose, Massachusetts paid nearly $500 to get back online.

"We are seeing an uptick in this type of activity," said Ari Mahairis, who heads the FBI's New York cyber division. "One of the reasons that our numbers are growing is because of the idea that people are paying the ransoms."

In 2014, the FBI received over 1,800 complaints about ransomware, an estimated loss of more than $23 million. In 2015, the bureau received over 2,400 complaints, and victims lost over $24 million.

"These are just the cases that are being reported. We suspect there are many more out there that haven't," Mahairis said.

The ransom demands are often relatively small -- hundreds to a few thousand dollars -- but the loss to an individual or business can be huge. "It's a very, very helpless feeling to open your computer and you don't have your computer anymore," Naraine said.

Naraine urges users to "back up" information for protection.

"Good user habits, common sense, backups and patching. With those basic things in place, I think you can minimize your exposure," Naraine said.