

Monthly Cybersecurity Newsletter

August 2019
Issue



Enterprise Security and Risk Management Office (ESRMO)

From the Desk of the State Chief Risk Officer – Maria Thompson



Ransomware Comeback!

Ransomware has become one of the most serious and prevalent cyber threats. Ransomware is a type of malicious software (malware), that encrypts a victim's files and systems, denying access to them, until a ransom has been paid. Ransomware can be much more serious than denying legitimate access to one's systems and files. It can deny hospitals access to needed files and resources or prevent cities from rendering needed public services. Despite reports released last year that predicted a decline in ransomware, these attacks have increased. According to one source, ransomware attacks on businesses rose over **500%** from 2018 to 2019. In response to this increase, the Cybersecurity and Infrastructure Security Agency (CISA) released its first CISA Insights product, [CISA Insights – Ransomware Outbreak](#), which includes recommendations to help organizations limit damage, and recover smartly and effectively.

Recently, a sophisticated ransomware attack, or series of attacks, infected the systems and data of 22 local government organizations in Texas and held them hostage for millions of dollars. Evidence currently points that these attacks came from a "single threat actor". According to several experts who are helping the Texas local government organizations, the vector of attack appears to have been through one trusted communications channel primarily used by law enforcement. Once the attack was inside that system, it was then able to propagate to other systems. State and federal authorities are assisting with the recovery of their systems and data.

More than 40 municipalities have been the victims of cyberattacks this year, ranging from major cities such as Baltimore and Albany, to smaller towns such as Lake City, Florida. Lake City and Rockville Center, N.Y. School District are among the few organizations hit with ransomware to have paid the ransom. They claim that rebuilding their systems would have been more costly. The Federal Bureau of Investigation (F.B.I.) warns, however, that paying the ransom in these cyber attacks only encourages more attacks and there is no guarantee the system and data will be recovered. Unfortunately, most ransomware attacks appear to target small-town America, probably because many local governments have fewer financial and technical resources and they are less likely to have updated their cyber defenses or backed up their data.

What Can You Do?

Some of the things you can do to help avoid becoming the next victim to ransomware includes the following actions:



- Think before you click! Never click on links or open attachments in unsolicited emails.
- Follow safe practices when browsing the Internet. Avoid questionable sites.
- Segment networks/devices. Make it harder for malware to infect multiple systems.
- Backup data, system images, and configurations regularly and keep the backups off the main network. Be sure to regularly test your backup and restoration process.
- Update and patch systems regularly. This eliminates known vulnerabilities.
- Make sure anti-malware and other security solutions are installed and up to date.
- Review and update as necessary disaster recovery plans and procedures.
- Review and exercise your incident response plan. Know how to respond and who to contact when an incident occurs.
- Pay attention to ransomware events and apply any lessons learned.
- If your organization is infected with ransomware, be sure to report it and ask for help in mitigating/responding to the incident.

How to Spot a Phishing Message

Phishing emails are still the most prevalent risks to the average computer user. The goal of a phishing email is to gain information about you, steal money from you, or install malware on your device(s). Phishing is also one of the most used ways to install ransomware, a cyber threat that is on the rise. So, what are some tell-tale signs of a phishing message? The following list includes some tips for spotting a phishing message.

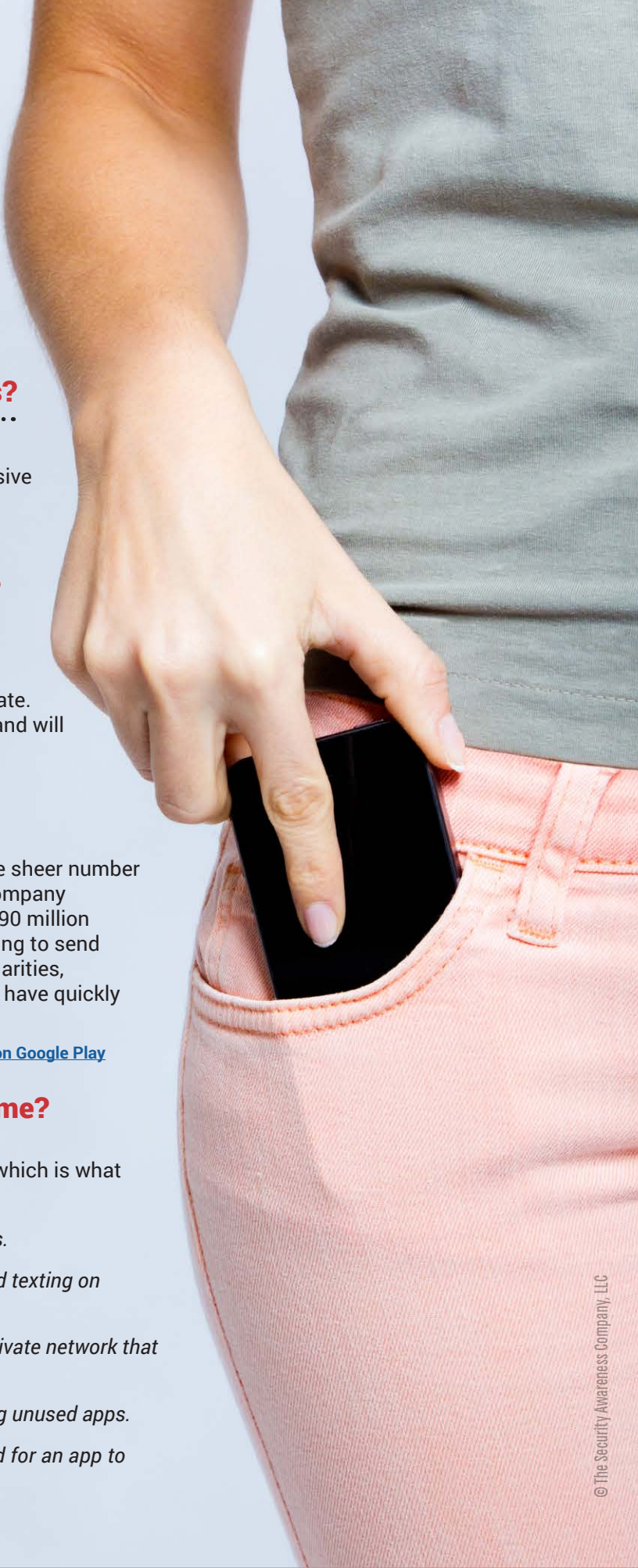


- Be suspicious of ALL unexpected emails.
- Don't trust the name or email address of the sender in the email. These can be spoofed.
- Verify links in a message before clicking them. Hover over a link to see where it will take you. Better, don't click on links at all; enter known good URLs in your browser software.
- Check for spelling/grammatical errors. Many phishing messages have poor spelling and grammar; however, phishing messages are getting more sophisticated!
- Look at the greeting. Is it general or vague?
- Is the email asking for personal information? Legitimate organizations will not request personal information via email.
- Is the email urgent? Phishing messages tend to elicit a sense of urgency.
- Check the email signature. While this can be forged, most legitimate senders will include a full signature with contact information.
- Be leery of attachments. If an unsolicited email requests you to open an attachment or download a file, contact the sender directly (not via email) and verify the message.

Remember...you may be one click away from divulging sensitive information or compromising your systems and data. Stop! Think! Connect!



The Threat in Your Pocket



Why do cybercriminals target smartphones?

The obvious answer: there are a lot of them. Estimates show that over 5.1 billion people own a smartphone. That's a massive target oozing with hacking potential.

Source: [BankMyCell.com Blog - How Many Phones Are In The World?](#)

What makes mobile devices so vulnerable?

Smartphones have screen-size limitations that restrict what can be viewed. For example, it's difficult to hover over links to show their full URL or to ensure that a webpage is legitimate. Also, people are easily distracted when using smartphones and will often click quickly, without much thought.







How common are mobile attacks?

App stores struggle to catch malicious developers due to the sheer number of new apps uploaded every day. Not long ago, a research company identified six malicious applications which already had over 90 million downloads. Furthermore, cybercriminals utilize text messaging to send malicious links while impersonating financial institutions, charities, government agencies, utility companies, etc. Mobile devices have quickly become one of the top attack vectors for cybercriminals.

Source: [Checkpoint Research Article - PreAMo: A Clicker Campaign found on Google Play](#)

What can we do to prevent mobile cybercrime?

First and foremost, treat your smart device like a computer, which is what it is. That means you need to be:

-  Utilizing antivirus software and enabling automatic updates.
-  Staying alert for phishing attacks, which come via email and texting on smartphones.
-  Never connecting to public WiFi without a VPN—a virtual private network that encrypts your connection.
-  Vetting all apps before downloading AND regularly removing unused apps.
-  Allowing only the minimum number of permissions needed for an app to properly function.
-  Always following our organization's mobile device policies.

CYBERSECURITY NEWSLETTERS

Security Awareness Newsletter: Monthly security awareness newsletter provided by KnowBe4 for all State employees.

Note: *You must have a valid State employee O365 account.*



- https://nconnect.sharepoint.com/sites/it_ext/esrmo_ext/Documents/Newsletters/Security%20Awareness%20News/2019

Security Tips Newsletter: Free monthly cybersecurity resource from the Center for Internet Security (CIS). This month the newsletter covers **Careers in Cybersecurity: Learn More or Get Involved!**

- <https://www.cisecurity.org/resources/?type=newsletter>

SANS OUCH! Newsletter: Free monthly cybersecurity awareness newsletter provided by The SANS Institute. This month's edition is titled **Got Backups?**

- <https://www.sans.org/security-awareness-training/ouch-newsletter>



Be A Cybersecurity Champion

National Cybersecurity Awareness Month (NCSAM) is almost here and the National Cybersecurity Awareness Month [Champion program](#) is a way to officially show your support for cybersecurity awareness. Champions represent those dedicated to making the connected world a safer place through awareness and education. Being a Champion is easy and does not require any financial support. NCSAM Champions include the following:

- Companies and organizations of all sizes
- Schools and school districts, colleges and universities
- Nonprofits
- Government organizations
- Individuals

Any individual or organization (state, local, private, etc.) can register to be an NCSAM Champion – it is easy and it is FREE! Organizations also have the opportunity to have their name listed on the NCSAM Champions website.

The National Cyber Security Alliance (NCSA) has provided more [information](#) and a webinar about this year's NCSAM theme and calls to action, how you and your organization can get involved and why you should register as a NCSAM 2019 Champion.



Penetration Testing: From a Hacker's Perspective

Coalfire, a PCI compliance validation services vendor, will be hosting a 1-hour webinar for the State of NC's merchant community on **September 3, 2019**. More information is below.

Date/Time: 9/3/2019 10:00am-11:00am EST

Webinar Description: Luke McOmie will discuss the importance of pentesting, stories from past assessments, and will step through the methodology and process of how Coalfire conducts blended threat, real world, impact and risk-based assessments (Red Teaming) and the importance it plays in securing modern businesses.

Join the webinar via <https://global.gotomeeting.com/join/694641885>.

You can also dial in using your phone: (571) 317-3116, Access Code: 694-641-885



ISSA Thought Leadership Series: Update on the latest cyber threats and trends

How protected are you from the latest types of DDoS attacks? One cyber threats report confirms that DDoS attacks continue to be an effective means of inflicting damage. An ISSA webinar will look at those findings:

- Growth and complexity of attacks
- Emerging new attack trends
- How to protect your online presence from new and evolving DDoS attacks
- Which cyber threats most concern senior IT security executives

The webinar will be on **September 11 @ 1pm**. Register to attend the webinar [here](#).

- **September** – [National Preparedness Month](#)
- **September 1** – Agency Compliance Reports Due
- **September 2** – Labor Day
- **September 4** – [Emergencies and Disasters: Are You Financially Prepared? Webinar](#), 1:00–1:30 PM Eastern Time
- **September 25** – [See Something, Say Something Awareness Day](#)
- **October** – [National Cybersecurity Awareness Month \(NCSAM\)](#)
- **October 10-11** – NC Cybersecurity Symposium

