NJCCIC
New Jersey Cybersecurity & Communications Integration Cell

THE WEEKLY BULLETIN

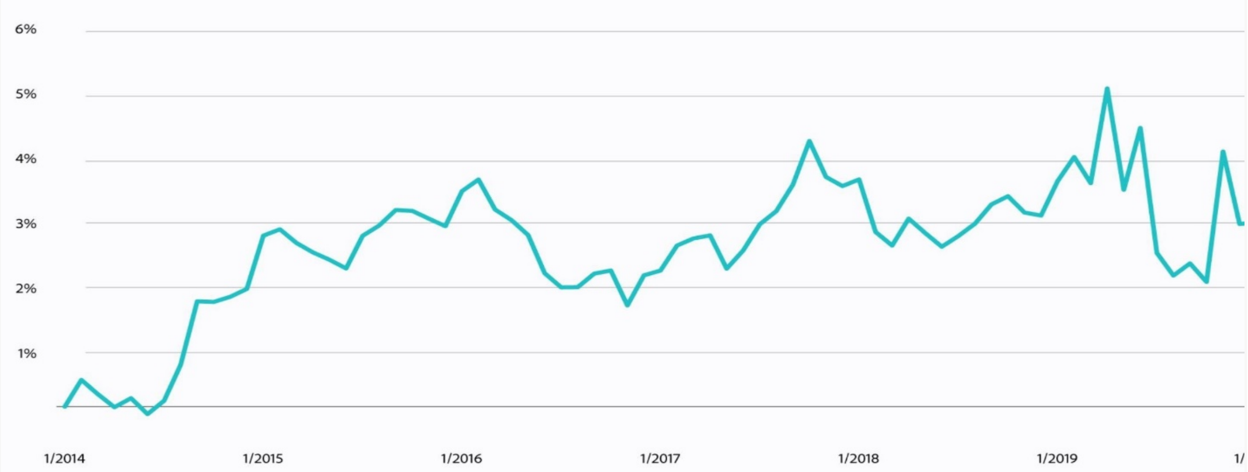
May 14, 2020

TLP: WHITE

Garden State Cyber Threat Highlights

Providing our members with a weekly insight into the threats and malicious activity directly targeting New Jersey networks.

Online Shopping and Cybersecurity

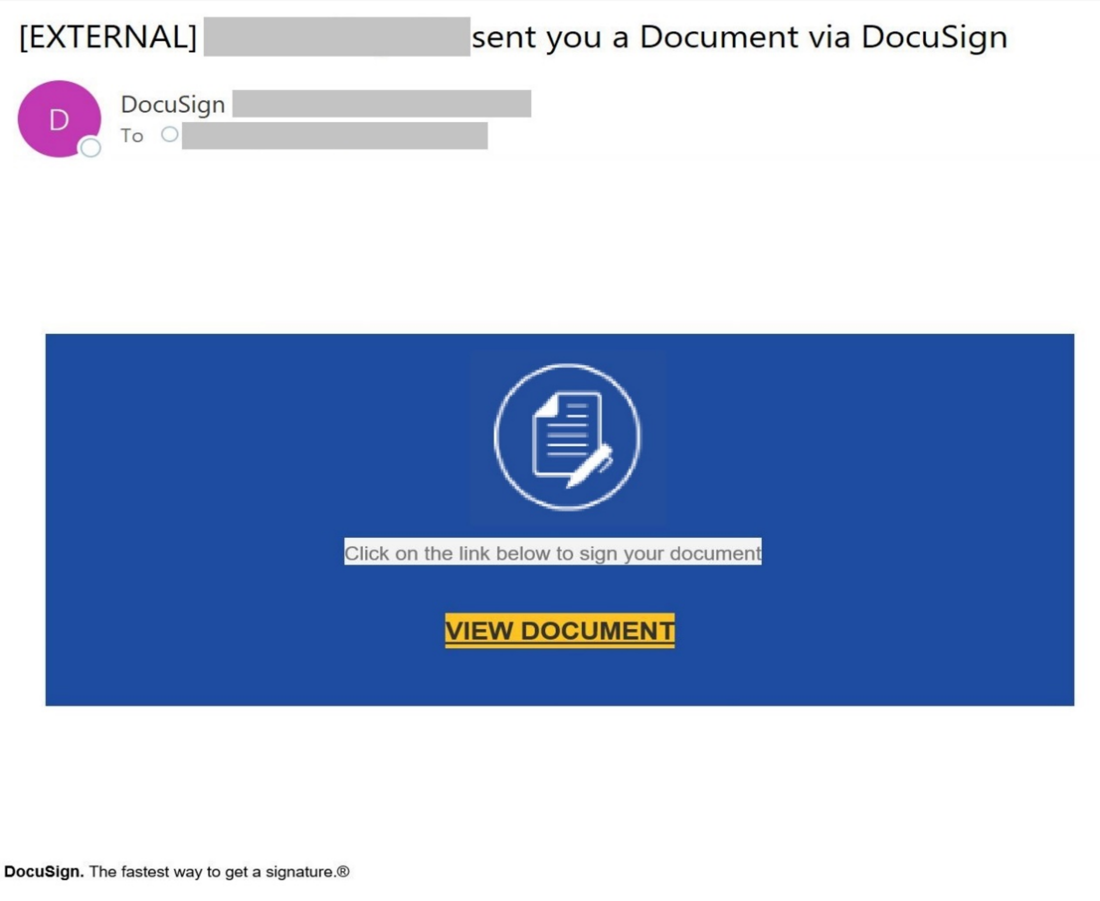


Online Grocery Price Changes | Digital Economy Index (U.S.)
Source: Adobe Analytics

Quarantine has forced many people to shop online more than ever in order to purchase items, from electronics to groceries. Some have been shopping online for years and apply best practices to do so securely; however, many people are new to this purchasing platform and could be increasing their risk for cybersecurity and identity theft incidents. According to Adobe's [Digital Economy Index](), online retail sales increased 49 percent between March and April 2020. Threat actors can target online shoppers through a variety of methods, including email, compromised websites, spoofed websites, and text-based phishing messages (known as SMiShing). When purchasing goods and services online, users are encouraged to follow best practices to reduce their risk of victimization.

The NJCCIC advises online shoppers to exercise caution with unsolicited emails that contain links or attachments advertising discounts on purchases or requesting verification of account information. Instead of clicking links in emails, navigate directly to websites by manually typing the URL into the browser. Additionally, we recommend using credit cards over debit cards for online purchases. Credit cards often have greater consumer protections that limit a victim's liability if fraudulent purchases are made. Magecart attacks – malicious code injected into online payment websites to steal financial data – are prevalent and pose a risk when online shopping. Lastly, the NJCCIC highly encourages all users to enable multi-factor authentication (MFA) on every account that offers it, including any online shopping websites. MFA significantly reduces a user's risk of account compromise via credential theft, increasing the user's resiliency to the unauthorized purchase of goods and services via a compromised account.

DocuSign Phishing Campaigns



[EXTERNAL] [redacted] sent you a Document via DocuSign

DocuSign [redacted]
To [redacted]

Click on the link below to sign your document

DocuSign. The fastest way to get a signature.®

DocuSign is a platform that provides secure electronic document signing, especially for important business documents. The NJCCIC's email security solution has identified and blocked multiple phishing campaigns, including those impersonating a notification from DocuSign with the intent to steal user credentials. The phishing email contains content and images of real emails from DocuSign, in an effort to appear legitimate to the recipient. The notification appears to be sent from "DocuSign" with a button to view the document that, if clicked, ultimately redirects the user to a spoofed DocuSign login page used to capture DocuSign credentials and the business email address associated with that account. Similar tactics and techniques are using the same layout with "Please DocuSign:" and keywords such as "contract" or "agreement" in the subject line, and the message appears to be from a specific person requesting the recipient to sign the document. Other sources have reported DocuSign phishing campaigns with COVID-19 themes, including COVID-19 Electronic Documents and US Department of Labor FMLA documents attempting to deliver TrickBot.

The NJCCIC recommends users and organizations educate themselves and others on these continuing threats and tactics to reduce victimization. Users are advised to avoid clicking links, opening attachments, or providing personal or financial information in response to emails from unknown senders and exercise caution with emails from known senders. If you are unsure of an email's legitimacy, contact the sender via a separate means of communication.

Announcements

FBI & CISA Release PSA on COVID-19 PRC Activity

The Federal Bureau of Investigation (FBI) and Cybersecurity and Infrastructure Security Agency (CISA) issued a Public Service Announcement to raise awareness of the threat to COVID-19-related research. The FBI is investigating the targeting and compromise of US organizations conducting COVID-19-related research by cyber actors affiliated with the People's Republic of China (PRC) and non-traditional collectors. These actors have been observed attempting to identify and illicitly obtain valuable intellectual property (IP) and public health data related to vaccines, treatments, and testing from networks and personnel affiliated with COVID-19-related research. The potential theft of this information jeopardizes the delivery of secure, effective, and efficient treatment options.

CISA, FBI, and DoD Release Information on Three Malware Variants Used by North Korea

CISA, FBI, and the Department of Defense (DoD) have identified three malware variants — COPPERHEDGE, TAINTEDSCRIBE, and PEBBLEDASH — used by North Korean government cyber actors, referred to as HIDDEN COBRA. In addition, US Cyber Command released the three malware samples to the malware aggregation tool and repository, VirusTotal. CISA encourages users and administrators to review the Malware Analysis Reports for each malware variant listed above, US Cyber Command's VirusTotal page, and CISA's North Korean Malicious Cyber Activity page for more information.

CISA Offers Free Assessments and Technical Services

CISA has introduced the National Cybersecurity Assessments and Technical Services resource in an effort to assist organizations in securing their networks during these unparalleled times. These services are available at no cost to federal agencies, state and local governments, and critical infrastructure – to include the healthcare sector, and private organizations. Users can find additional details and sign up for these services here.

Industry Reports

Risk Based Security

RiskBased SECURITY

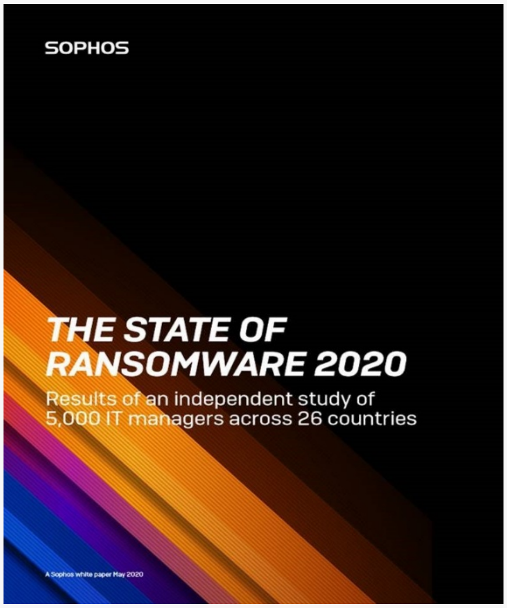
2020 Q1 Report

Data Breach QuickView

Risk Based Security released the 2020 Q1 Data Breach QuickView Report, which highlights data breach trends in 2020 and the impact of the COVID-19 pandemic. Cybercrime is expected to increase during this pandemic, including compromised systems due to remote work, phishing attacks due to distracted or vulnerable targets, and limited resources addressing issues and incidents due to security budget cuts. Below are some key takeaways:

- The number of publicly reported breaches in Q1 2020 decreased by 58 percent compared to Q1 2019, due to reporting disruptions caused by the pandemic and the unusually high number of reported breaches in Q1 2019.
- The number of records exposed in Q1 2020 dramatically increased by 273 percent to 8.4 billion compared to Q1 2019, due to a misconfigured ElasticSearch cluster exposing 5.1 billion records.
- Aside from the ElasticSearch incident, the number of records still increased by 48 percent in Q1 2020 compared to Q1 2019.
- Approximately 70 percent of reported breaches were a result of unauthorized access to systems or servers.
- Approximately 90 percent of records exposed were a result of exposing or publishing data online.
- Most breaches originated from outside the organization and insider breaches were more often accidental than malicious.
- Eleven breaches exposed more than 100 million records each and five breaches exposed between 10 and 99 million records.
- Approximately 68 percent of the breaches with confirmed record counts exposed fewer than 1,000 records.
- Email, password, and name were the top data types exposed in breaches.
- The highest number of reported Q1 2020 breaches were in the healthcare, information, and public administration sectors.

Sophos



SOPHOS

THE STATE OF RANSOMWARE 2020

Results of an independent study of 5,000 IT managers across 26 countries

A Sophos white paper May 2020

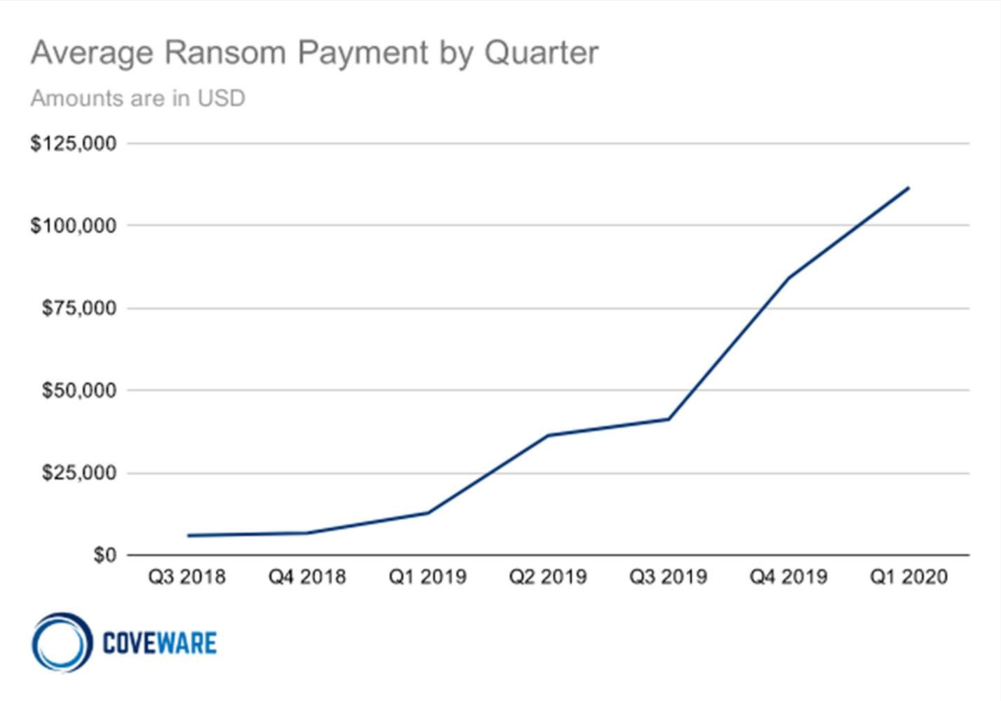
Sophos released The State of Ransomware 2020, an independent study in which 5,000 information technology managers ranging from SMBs to large corporations were surveyed across 26 countries. The study provides comprehensive insight into the experiences of organizations impacted by ransomware attacks. Below are some key takeaways:

- Of the average (51 percent) number of organizations that suffered a ransomware attack over the last year, 73 percent resulted in data encryption; the number of US organizations that suffered attacks was slightly above average at 59 percent.
- 94 percent of organizations were able to successfully restore data after encryption, with 26 percent paying the ransom, and twice as many (56 percent) restoring from backups.
- The average cost of ransomware attacks – to include downtime, costs of device replacement and network scrubbing, and lost business opportunities – doubled from an average of $732,520 to $1,448,458 when organizations paid the ransom.

- 59 percent of attacks in which data was encrypted involved public cloud data, with 41 percent of encrypted data from on premise and private cloud.
- 84 percent of those surveyed have cybersecurity insurance; however, only 64 percent of those insured have ransomware coverage.
- Of the organizations that have ransomware coverage, 94 percent paid the ransom through their insurance company.
- Of those surveyed, 51 percent were victims of ransomware, a slight decrease from previous years. This drop is likely due to a change in tactics, in which threat actors have begun to focus on highly targeted server-based attacks that require more effort to deploy.
- 45 percent of public sector respondents, 60 percent of media, leisure, and entertainment respondents, and 56 percent of IT, technology, and telecom respondents were victims of ransomware attacks. While it is assumed that the public sector is highly targeted by ransomware attacks due to widespread public attention, these organizations appear to be less impacted, according to this survey.

Threat Alerts

Ransomware in the Time of COVID-19



While businesses and organizations are still struggling to establish work-from-home accommodations and keep their operations running, cyber threat actors have not faltered. Ransomware incidents continue with business as usual, targeting small and medium-sized businesses and large corporations alike. In just the last week, ATM provider Diebold Nixdorf, media and entertainment law firm Grubman Shire Meiselas & Sacks, Pitney Bowes, and the Texas Office of Court Administration all publicly acknowledged ransomware attacks on their networks. In the case of Grubman and Pitney Bowes, the threat actors stole data from the network prior to encryption, an increasingly popular tactic employed by threat actors in an attempt to force victims to pay ransom demands to prevent disclosure of the stolen data. The Ako ransomware variant increased its extorting attempts by demanding two ransoms, one for file recovery and one to not publish stolen data. Ransomware demands have also greatly increased. Coveware reported that the average ransom demand increased to over $110,000 in Q1 2020, up from $87,000 in Q4 2019. Businesses and organizations in New Jersey have also been victimized by ransomware in recent weeks, further complicating operations in a state severely impacted by COVID-19.

The NJCCIC recommends businesses and organizations follow ransomware risk mitigation strategies to reduce their risk of a ransomware infection and ensure they have a comprehensive data backup plan in place that includes keeping multiple, tested copies offline with at least one in a separate and secure location.

Ramsay Malware Can Steal from Air-Gapped Systems

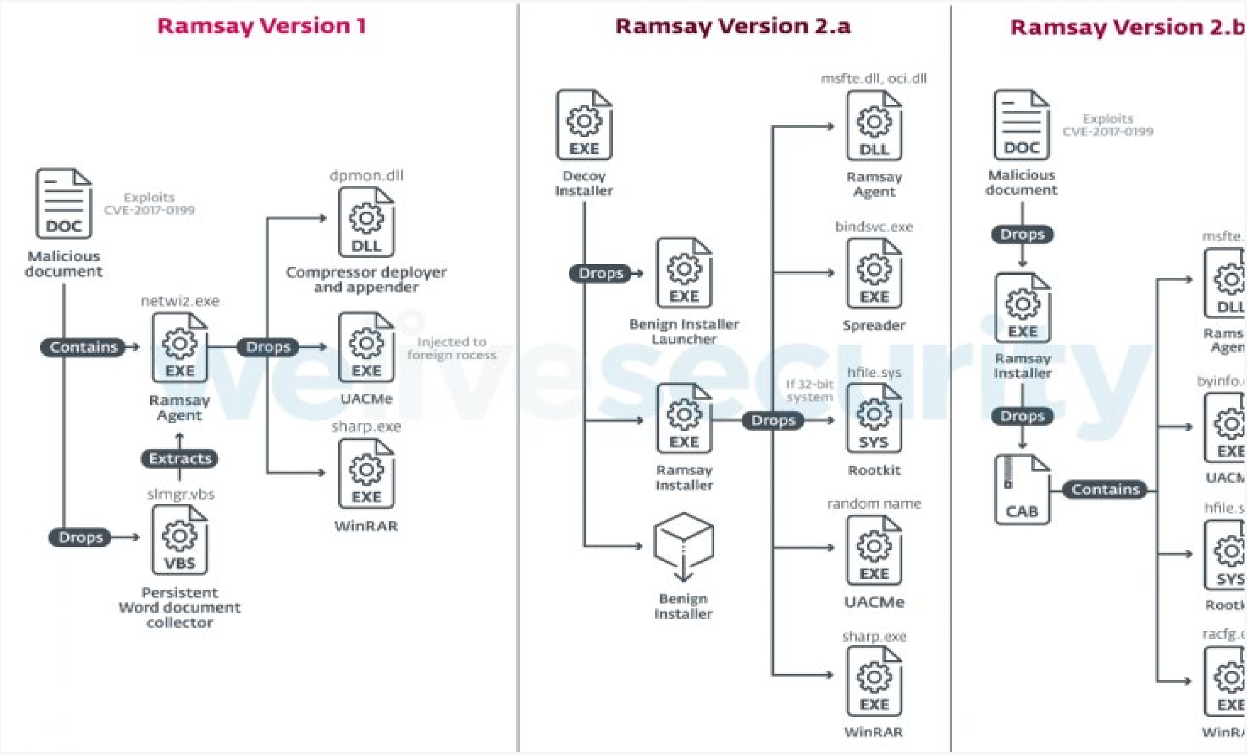


Image Source: ESET

Air-gapped systems are computers or networks isolated from an organization's network and the public internet as they typically contain highly-sensitive data, such as classified documents or intellectual property. ESET researchers discovered three different versions of a new, developing malware framework, dubbed Ramsay, that can jump the air gap to infect these isolated systems and collect sensitive documents to a hidden container for exfiltration at a later time. Other features include a rootkit and spreader component that appends copies of the Ramsay malware to all portable executable (PE) files on removable drives and network shares, which is presumed to be the mechanism used to jump the air gap.

The NJCCIC recommends users adopt a defense-in-depth cybersecurity strategy, keep systems patched and up to date, and maintain cybersecurity best practices, including physical security. Additional technical information, including attack vectors, capabilities, and Indicators of Compromise (IoCs), can be found in the ESET article and the ZDNet article.

Vulnerability Advisories

Thunderbolt Vulnerabilities Affect Millions of Devices

Researcher Björn Ruytenberg discovered several vulnerabilities in Thunderbolt-equipped systems, including Mac, Linux, and Windows devices. Threat actors could exploit these vulnerabilities by reading and copying data with brief physical access to the system, a screwdriver, and easily portable hardware to access system memory — even if the device has full disk encryption, Secure Boot, strong BIOS and operating system account passwords, and other best practices employed. Remediating the vulnerabilities would require a silicon redesign; however, there is a Spycheck tool to verify affected systems before following the recommendations provided by Spycheck.

The NJCCIC recommends users adopt a defense-in-depth cybersecurity strategy and maintain cybersecurity best practices, including physical security. More detailed information and demo can be found in the Thunderspy report and the ZDNet article.

VMware vRealize Operations Manager Impacted by SaltStack Vulnerabilities

Two vulnerabilities discovered in SaltStack's Salt project, authentication bypass vulnerability CVE-2020-11651 and directory traversal vulnerability CVE-2020-11652 , affect the Application Remote Controller (ARC) in VMware vRealize Operations Manager. Exploitation of CVE-2020-11651 could allow a threat actor to take control of the ARC and any virtual machines in the ARC with a Telegraf agent, and exploitation of CVE-2020-11652 could allow a threat actor to access the entire ARC filesystem. Updates to mitigate the vulnerabilities are forthcoming.

The NJCCIC recommends users and administrators of VMware's vRealize Operations Manager apply the [workarounds]() provided by VMware and apply updates when they become available after appropriate testing. More information can be found in the [VMware Security Advisory]().

Breach Notification

Kunst Bilder/Shutterstock.com

Microsoft GitHub

A hacking group known as Shiny Hunters stole 500 GB of data from Microsoft's private GitHub repositories. The group, who gained access through a compromised employee account, published some of the stolen projects on a hacking forum that contained various files, directories, and some private Microsoft GitHub projects. Researchers assess that Shiny Hunters gained access to roughly 1,200 private repositories around March 28, 2020, which have since been secured. Though the breach was largely dismissed as insignificant, some images of the directory listing appear to contain source code for Azure, Office, and some Windows runtimes, and concerns have been raised regarding access to private API keys or passwords that may have been mistakenly included in some private repositories. Additionally, Shiny Hunters is flooding dark web marketplaces with breached databases, selling an estimated 73.2 million user records from at least 11 different breached companies just this week. Users are urged to establish strong passwords, unique to each site, and enable multi-factor authentication where available. Further information can be found in the ZDNet article.

Threat Profiles

Android | ATM Malware | Botnet | Cryptocurrency-Mining | Exploit Kit

Industrial Control Systems | iOS | macOS | Point-of-Sale | Ransomware | Trojan

ICS-CERT Advisories

3S-Smart Software Solutions GmbH CODESYS V3 (Update A)

3S-Smart Software Solutions GmbH CODESYS V3 Library Manager (Update A)

Eaton Intelligent Power Manager

Emerson WirelessHART Gateway

Interpeak IPnet TCP/IP Stack (Update D)

Opto 22 SoftPAC Project

OSIsoft PI System

Siemens KTK, SIDOOR, SIMATIC, and SINAMICS (Update A)

Siemens RUGGEDCOM, SCALANCE, SIMATIC, SINEMA (Update A)

Siemens SIMATIC PCS 7, SIMATIC WinCC, and SIMATIC NET PC (Update C)

Siemens SINAMICS (Update C)

Siemens SIPROTEC 5 and DIGSI 5 (Update C)

Patches	Throwback Thursday
Adobe | Microsoft	The Internet of Insecure Things
SAP | vBulletin	

Social Engineering Awareness

Are You Sure You Would Never Fall for a Phishing Scam?

Comment: The recent increase in phishing scams has brought attention to the cyber threat landscape. Users may perceive others as more likely than themselves to fall for phishing scams, creating false confidence in their own sense of security. Users may not truly assess their own behaviors and actions, thus potentially increasing the likelihood of being victimized. To reduce victimization and jeopardizing both users and their employers, security awareness training and phishing simulations can help to identify and assess risk as well as reinforce confidence in online safety.

Cyber at a Glance

Home Workplaces Introduce New Risk, Poor Password Hygiene

Comment: Working from home and remotely connecting to corporate networks and resources have introduced new risks, such as distractions, use of personal devices, and poor password hygiene. Cyber-criminals are taking advantage of these risks with increased phishing scams and other attacks. Users are advised to use company-issued assets (where available), avoid sharing devices with family members, and refrain from conducting personal business on work systems. It is also recommended to create strong and unique passwords, change them frequently, keep them private, and enable multi-factor authentication where available to reduce the risk of account compromise.

The information contained in this product is marked Traffic Light Protocol (TLP): WHITE. Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.

TLP: WHITE

Questions?

Email a Cyber Liaison Officer at njccic@cyber.nj.gov.

The Weekly Bulletin aggregates information about cyber threats, vulnerabilities, and other resources to promote shared awareness and the adoption of best practices. Designed for a general audience, the Bulletin aims to bridge the information sharing gaps between all levels of government, the private sector, and our citizens.

Connect

Share

This email was sent by:

New Jersey Cybersecurity & Communications Integration Cell

DISCLAIMER: This product is provided as is for informational purposes only. The New Jersey Cybersecurity & Communications Integration Cell (NJCCIC) does not provide any warranties of any kind regarding any information contained within. The NJCCIC does not endorse any commercial product or service, referenced in this product or otherwise. Further dissemination of this product is governed by the Traffic Light Protocol (TLP). For more information about TLP, see ***https://www.us-cert.gov/tlp***.