



# NJCCIC

NJ CYBERSECURITY & COMMUNICATIONS INTEGRATION CELL

## *THE WEEKLY BULLETIN | August 19, 2015*

---

### **E-ZPass Alert**

**August 19, 2015**

The Port Authority of New York and New Jersey has issued a warning about an email phishing scam that is currently targeting E-ZPass users. The New Jersey branch of E-ZPass released the following statement regarding the scam: "New Jersey drivers should know that legitimate toll violation notices are sent by mail, not email, from the E-ZPass Customer Service Center in Newark, NJ. The web address for paying a legitimate violation to agencies in the New Jersey E-ZPass Group is [www.EZPassNJ.com](http://www.EZPassNJ.com)."

[Read Full Alert Here](#)

---

### **NJ CyberLog**

**August 19, 2015**

[Public Wi-Fi -- Sacrificing Security For Convenience](#)

Using public Wi-Fi hotspots can be very risky without taking the proper precautions. There are several ways in which hackers can use these unsecured Wi-Fi signals to compromise devices and steal personal or financial data from unsuspecting victims. However, by being informed and taking the necessary steps to protect your data, you can still enjoy the convenience of a free and open Wi-Fi signal without sacrificing your security.

---

### **Tip of the Week**

#### ***"Cybersecurity Tips for Small Business"***

1. Establish basic security practices and policies for employees, such as requiring strong passwords, and establish appropriate internet use guidelines.

### **Latest NJCCIC Alerts**

[Vulnerability in Microsoft Internet Explorer Could Allow Remote Code Execution](#)

[Multiple Vulnerabilities in Apple Products](#)

[Vulnerability in Lenovo Service Engine \(LSE\) Could Allow Remote Code Execution](#)

---

2. Having the latest security software, web browser, and operating system are the best defenses against viruses, malware, and other online threats.
3. Regularly backup the data on all computers.
4. Work with banks or processors to ensure the most trusted and validated tools and anti-fraud services are being used.
5. Do not provide any one employee with access to all data systems. Employees should only be given access to the specific data systems that they need for their jobs.

## NJCCIC Announcements

**August 26 | 11am - 12pm E.S.T.**

[#NJOHSPwebinar | Cyber Threats Update from the NJCCIC](#)

This webinar will be conducted by cyber analysts from the NJCCIC, talking about cyber threats and security continuing to dominate the news as data breaches, doxing attacks and other attack methods targeting government, private sector and individual victims.

---

## Questions?

Email a Cyber Liaison Officer at  
[njccic@cyber.nj.gov](mailto:njccic@cyber.nj.gov)

---

## Connect with us!



---

[cyber.nj.gov](http://cyber.nj.gov)

## New Jersey Cybersecurity & Communications Integration Cell

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

Share this email:



[Manage](#) your preferences | [Opt out](#) using **TrueRemove™**

Got this as a forward? [Sign up](#) to receive our future emails.

View this email [online](#).

communications@njohsp.gov

Trenton, NJ | 08625 US

This email was sent to kmiscia@montclairnjusa.org.

*To continue receiving our emails, add us to your address book.*

