NYC EMERGENCY MANAGEMENT DEPARTMENT
NYC.gov/emergencymanagement
Press Office: 718-422-4888

For Immediate Release
#76-19

NATIONAL CYBERSECURITY AWARENESS MONTH: A REMINDER TO SAFEGUARD YOUR PERSONAL INFORMATION ONLINE

October 8, 2019 — National Cybersecurity Awareness Month, held every October, raises awareness of the importance of cybersecurity and encourages Americans to take steps to prevent cyber incidents at home and in the workplace. According to the U.S. Department of Homeland Security, 3.48 billion people now use social media worldwide. Whether you are updating your latest social media posts, surfing the web, or paying a bill, it is important that you take the necessary measures to protect your information.

Cyberattacks are malicious attempts to access or damage a computer system. Cyberattacks can lead to loss of money, theft of personal information, as well as damaged reputation and safety, and disrupt business and infrastructure. Eric Smalls, assistant commissioner of technology at New York City Emergency Management, encourages individuals to understand that a cyberattack is an emergency.

"We live in a digital age, and America is one of the most connected countries in the world. That connectivity means that we are open to cyber threats from anywhere in the world," **Smalls** said. "National Cybersecurity Awareness Month is important because it emphasizes the need to protect ourselves online. It highlights vulnerabilities and provides prevention tools and options individuals can use to stay safe online."

To help City agencies defend against cyber threats, New York City established NYC Cyber Command. NYC Cyber Command directs citywide cyber defense and incident response, mitigates cyber threats, and provides guidance to the Mayor and City agencies. Using the latest technologies and leveraging public-private partnerships, NYC Cyber Command works across more than 100 agencies and offices to protect, detect, respond, and recover from threats while setting citywide information security policies and standards.

NYC Cyber Command also works to help every-day New Yorkers protect their information online. In 2018, the agency launched the NYC Secure App, designed to defend New Yorkers from malicious cyber activity on mobile devices across public Wi-Fi networks. The NYC Secure app issues warnings to users when suspicious activity is detected on their mobile devices, and offers recommendations on how to address the threat.

New York City has strengthened its own Wi-Fi networks as well, implementing a new layer of security. The innovative technology protects users browsing the internet on City guest wireless networks from downloading malicious software such as ransomware, or accessing phishing websites that attempt to trick users into providing sensitive information such as usernames, passwords, or credit card details.

While New York City agencies work round-the-clock to prevent cyber threats, individuals must take steps to safeguard their information, whether at home or in the office. The first step to preventing a cyberattack is the ability to identify one when you see it.

Two common cyber threats are phishing and man-in-the-middle. Phishing utilizes human interaction to obtain or compromise information, using emails or malicious websites to solicit personal information by posing as a trustworthy organization. They are particularly popular during epidemics and health scares, holidays, and immediately following a natural disaster because they target individual vulnerabilities.

Phishing can also include the spread of harmful malware. The threats involve sending fraudulent emails instructing users to click links, which download harmful viruses and spyware that can compromise your information. If you doubt the legitimacy of an email or website, avoid clicking on any links.

A man-in-the-middle attack can occur when third parties insert themselves into a two-party transaction online. As you are typing, a bad actor is capturing your sensitive information including usernames, passwords, and credit card details. Man-in-the-middle attacks are particularly dangerous because users may have no idea their information is being stolen.

The cause of man-in-the-middle cyberattacks are often malware already installed on a device or the use of unsecure public Wi-Fi networks. Unsecure networks present challenges because attackers can insert themselves between your device and the network, stealing your personal information as you type. You should never share sensitive information on an unsecured Wi-Fi network.

Phishing and man-in-the-middle are two common threats, but there are steps you can take to protect yourself from other cyber threats. The best way to stay safe online is to be proactive. Ensure that software and operating systems on your home computer and devices are up-to-date and include antivirus solutions, anti-malware, and firewalls to block potential threats. Experts also suggest routinely backing up files on a cloud service or hard drive in case a cyberattack compromises your device. It is also important to protect your Wi-Fi network. If hackers access your Wi-Fi network, they can steal crucial personal information: be sure to protect it with a strong password.

“Passwords are as important as locking your front door. You wouldn’t secure your front door with a screen door that someone could just easily kick open,” **Eric Smalls said on a recent episode of NYC Emergency Management’s podcast “Prep Talk”.** “You want to have a real door with a real lock. Creating a complex password is securing your perimeter; you’re securing your private information.”

If you feel you have been a victim of a cyberattack, take steps to limit the damage. Change passwords for all online accounts and monitor your finances for unauthorized purchases. If the attack occurred at work, immediately inform your company’s IT department.

National Cybersecurity Awareness Month is an opportunity to take steps to help safeguard your personal information. As the frequency and complexity of cyber threats continue to increase, it is more important than ever to stay vigilant online. For more information on staying safe online visit, https://www1.nyc.gov/site/em/ready/cybersecurity.page.

'PREP TALK' PODCAST

On the latest episode of "Prep Talk," NYC Emergency Management's podcast, guests from New York City Emergency Management and the Department of Information Technology and Telecommunications (DoITT) raise awareness about the importance of cybersecurity. This year's theme — Own It, Secure It, Protect It — focuses on key areas including citizen privacy, consumer devices, and e-commerce security. The guests provide tips and resources to help individuals become safer online. You can listen to the latest episode on SoundCloud, iTunes and Spreaker.

###

Tashawn Brown is the press assistant at the New York City Emergency Management Department, where he has responded to various disasters and emergencies. As press assistant, he assists the department in day-to-day press operations and serves as one of the agency's spokespersons, helping to develop and distribute information to the news media. He has been at the forefront of expanding the reach of New York City Emergency Management, connecting with relevant academic and trade publications to promote agency content. Prior to joining NYC Emergency Management, he worked as a research analyst at The City of New York, Mayor's Office of Media and Research Analysis. The author can be reached at (718) 422-4888.