Subject: Security Alert: USB Devices
Date: February 2022

The FBI issued a warning of a cybercrime campaign in which **attackers mail USB thumb drives to US organizations with the goal of delivering ransomware into their environments**.

The FBI has observed a cybercriminal group known as FIN7 targeting the US defense industry with a package containing a fraudulent thank you letter, counterfeit Amazon gift card, and a USB device. When plugged into a computer system, the USB device automatically injects a series of keystrokes to download ransomware, bypassing common security controls.

Does this Sound Familiar?

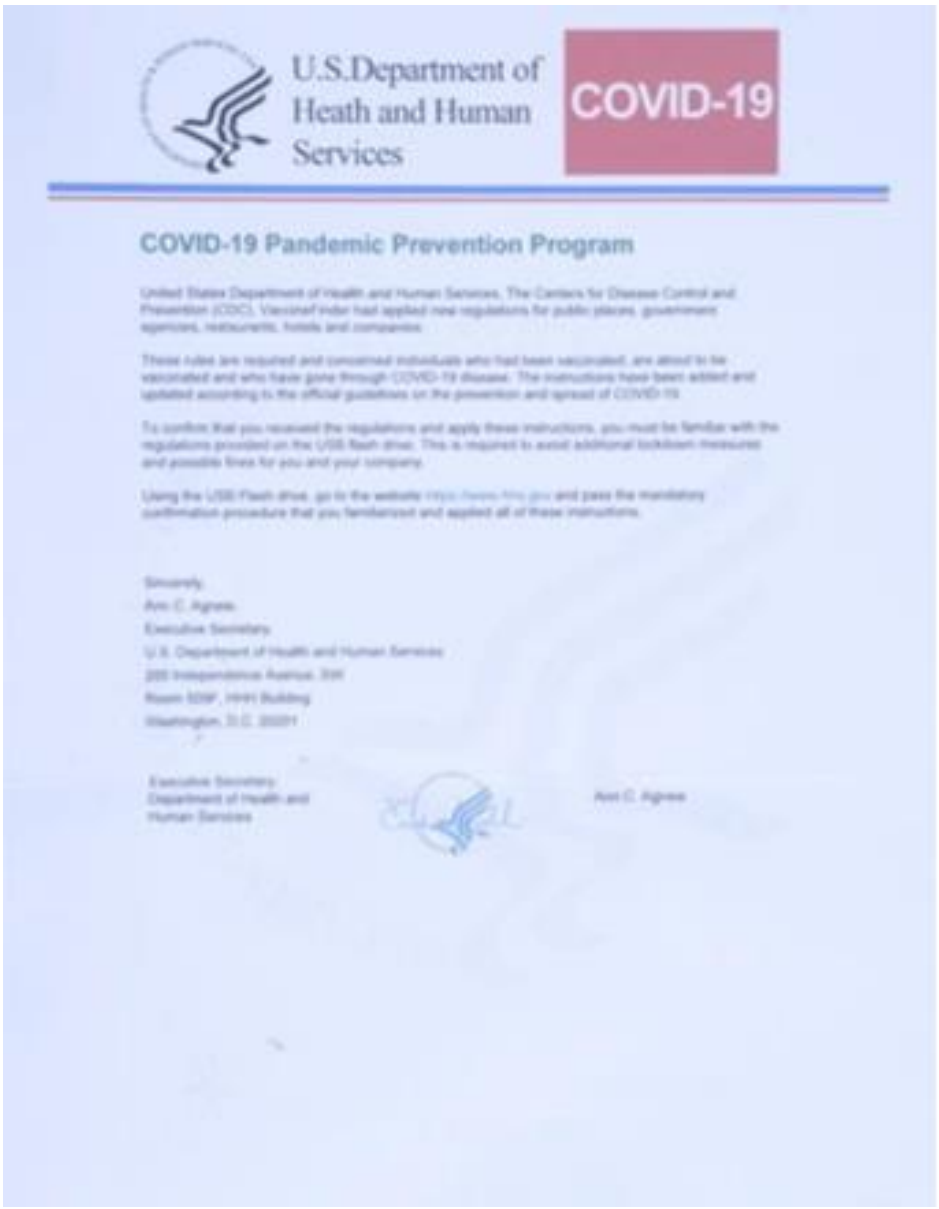
Similar to phishing emails, attackers use fraudulent messaging to take advantage of the recipient by preying on stress levels, curiosity, or hoping our guard is down. In this case, the intent is to pressure the recipient to plug the USB device into their computer.

Remember to trust your instincts, be cautious, and when in doubt, reach out to the IT Service Desk.

What to Look For:

Reports of these malicious packages have included two variations, both accompanied by the malicious USB devices:

1. Letters imitating the US Department of Health and Human Services (HHS) and providing information on COVID-19 guidelines, accompanied by a USB device.



U.S.Department of Heath and Human Services

COVID-19

COVID-19 Pandemic Prevention Program

United States Department of Health and Human Services, The Centers for Disease Control and Prevention (CDC), Vaccinef Index had applied new regulations for public places, government agencies, restaurants, hotels and companies.

These rules are required and concerned individuals who had been vaccinated, are about to be vaccinated and who have gone through COVID-19 disease. The instructions have been added and updated according to the official guidelines on the prevention and spread of COVID-19.

To confirm that you received the regulations and apply these instructions, you must be familiar with the regulations provided on the USB flash drive. This is required to avoid additional lockdown measures and possible fines for you and your company.

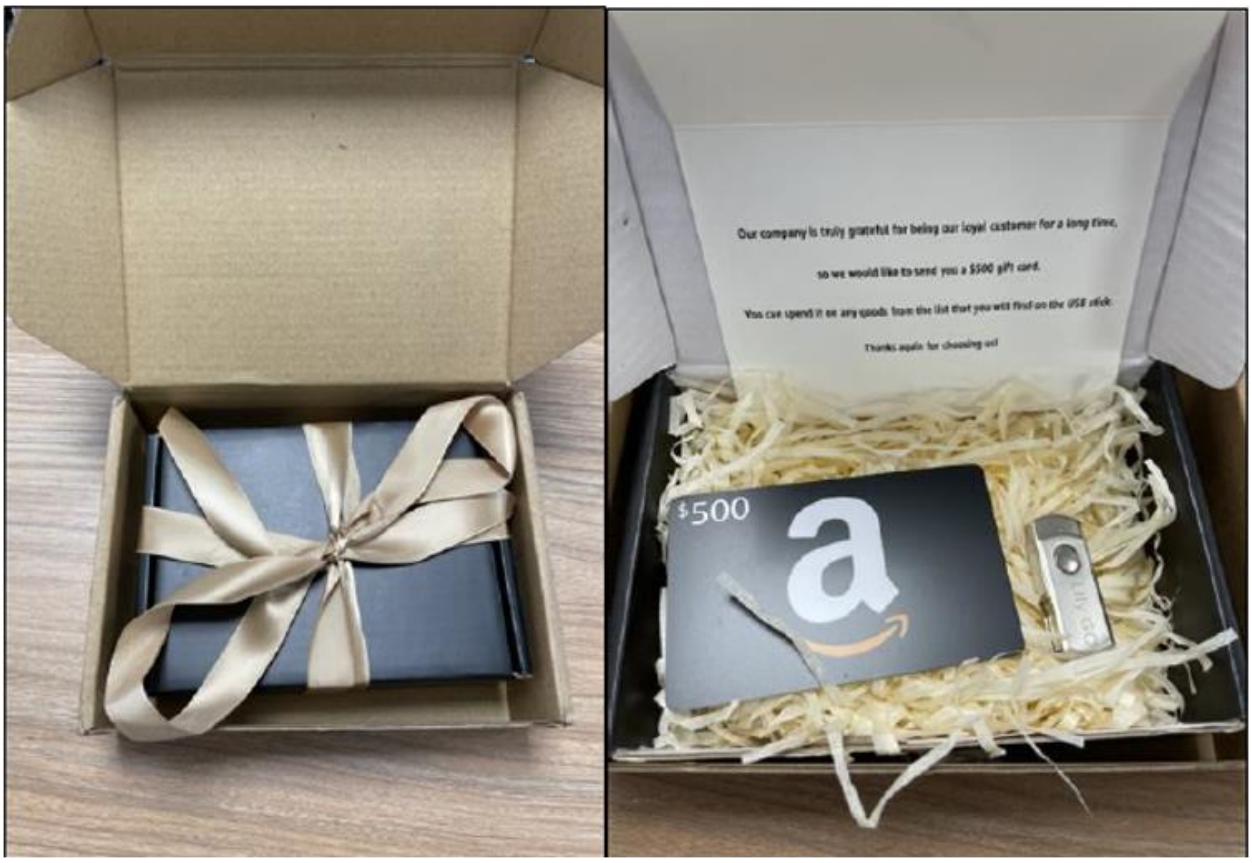
Using the USB Flash drive, go to the website https://www.hhs.gov and pass the mandatory confirmation procedure that you familiarized and applied all of these instructions.

Sincerely,
Ann C. Agnew
Executive Secretary
U.S. Department of Health and Human Services
200 Independence Avenue, SW
Room 509F, HHH Building
Washington, D.C. 20201

Executive Secretary
Department of Health and Human Services

Ann C. Agnew

2. Fake gifts with forged Amazon thank you cards and counterfeit gift cards.



The malicious USB devices are often LilyGo, as shown below.

USB Security Risks

USB drives, also known as thumb drives, are small, inexpensive, portable devices making them an easy choice for storing and transporting files from one computer to another. These features also make USB drives appealing to attackers.

Attackers can use USB drives to infect computers with malware that can detect when the USB drive is plugged into a computer. The malware then downloads malicious code onto the drive.

USB drives can be easily lost or stolen and if the information on the drive is not encrypted, anyone who has the USB drive can access the contained data.

How can you protect your data?

- **Never plug an unknown USB drive into your computer.** If you find a USB drive, do **not** plug it into your computer to view the contents. Contact the IT Service Desk for guidance.
- **Enable security features.** Use passwords and encryption on your USB drive to protect your data, and make sure that you have the information backed up in case your drive is lost.
- **Keep personal and business USB drives separate.** Do not use personal USB drives on computers owned by your organization, and do not plug USB drives containing corporate information into your personal computer.

If you have any questions or concerns, please contact the IT Service Desk:

- by email at itservicedesk@montgomerycollege.edu
- by web chat on OIT's web page
- by phone at 240-567-7222

Please do not reply to this email, as this mailbox is not monitored. Thank you.

IT Communications
Office of Information Technology