FRED UPTON, MICHIGAN
CHAIRMAN

FRANK PALLONE, JR., NEW JERSEY
RANKING MEMBER

ONE HUNDRED FOURTEENTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON ENERGY AND COMMERCE
2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6115
Majority (202) 225–2927
Minority (202) 225–3641

November 3, 2016

The Honorable Edith Ramirez
Chairwoman
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, D.C. 20580

Dear Chairwoman Ramirez,

We write to urge the Federal Trade Commission (FTC) to act to protect consumers from insecure Internet of Things (IoT) devices, particularly in light of the recent cyberattack that caused significant outages on many highly trafficked websites. First, the FTC should call on IoT device manufacturers to implement security measures, including patching vulnerabilities and requiring consumers to change the default passwords on devices during the set-up process. Second, the FTC should alert consumers to the security risks posed by continuing to use default passwords on IoT devices.

IoT devices played an integral role in the October 21, 2016, distributed denial of service (DDoS) attack that caused major internet outages across the country.[1] Mirai, the botnet used in the attack, was designed to scan the internet for poorly secured devices.[2] It was able to connect to nearly 400,000 IoT devices using a list of only 60 default usernames and passwords.[3] These devices then produced a large volume of junk traffic, leaving popular websites inaccessible to legitimate users.[4]

---

[1] *Hacked Cameras, DVRs Powered Today's Massive Internet Outage*, Krebs on Security (Oct. 21, 2016).

[2] *IoT Botnet Highlights the Dangers of Default Passwords*, Computer World (Oct. 3, 2016).

[3] *Id.*

[4] *Hacked Cameras, DVRs Powered Today's Massive Internet Outage*, Krebs on Security (Oct. 21, 2016).

IoT devices are the fastest growing category of connected devices compared to other categories such as smartphones, tablets, and televisions.[5] A recent report predicted that between 2015 and 2020, the number of IoT connections will grow nearly 2.5-fold, from 4.9 billion in 2015 to 12.2 billion in 2020.[6] By 2020, IoT devices will account for nearly half of all connected devices.

Consumers have concerns about the security of connected devices. A recent survey found that more than 40 percent of consumers are not confident that IoT devices are safe and able to protect their personal information.[7] Yet, many consumers are not implementing basic precautions to protect their own devices. For example, nearly 50 percent of consumers recently surveyed reported that they were either unaware of or had chosen not to change the default passwords on their home routers.[8]

Most consumers whose IoT devices were used in the recent DDoS attack or similar attacks will never know that their devices were accessed.[9] Without their owners' knowledge, unsecured devices allow hackers to control their use and possibly learn private information about their owners. For example, a hacker may hijack a consumer's home web camera to learn intimate details of what is going on within the owner's residence.

It is highly probable that these types of cyberattacks will continue and become more common. Security experts have warned that although the recent DDoS attack was historic given the technical capabilities employed and the volume of devices exploited, similar disruptions will likely occur in the future.[10] Additionally, more botnets like Mirai that take advantage of weak default passwords will appear if IoT device manufactures do not take action.[11]

To address this issue, several IoT device manufacturers have started requiring users to create unique passwords for their devices.[12] The FTC has also previously commented on the security risks posed by default passwords. In an August 2013 article on using IP cameras safely,

---

[5] *IoT Will Account for Nearly Half of Connected Devices by 2020, Cisco Says*, ZDNet (June 7, 2016).

[6] *Id.*

[7] ESET, *Our Increasingly Connected Lives* (Oct. 24, 2016) (online at cdn3.esetstatic.com/eset/US/resources/press/ESET_ConnectedLives-DataSummary.pdf).

[8] *Id.*

[9] *IoT Growing Faster Than the Ability to Defend It,* Scientific American (Oct. 26, 2016).

[10] *Friday's IoT-based DDoS Attack Has Security Experts Worried,* Computer World (Oct. 25, 2016); *What We Know About Friday's Massive East Coast Internet Outage*, Wired (Oct. 21, 2016).

[11] *IoT Botnet Highlights the Dangers of Default Passwords*, Computer World (Oct. 3, 2016).

[12] *Who Makes the IoT Things Under Attack?*, Krebs on Security (Oct. 16, 2016).

the Commission encouraged consumers to change from the default username and password.[13] In a January 2015 report, the Commission noted that device manufacturers should require consumers to change the default password during set-up.[14]

While the FTC's past warnings are commendable, they are insufficient in the current environment. The FTC has published no additional warnings or advice to consumers in light of the October 21 DDoS cyberattack. An incident that security experts have labeled "historic" coupled with the rapid proliferation of IoT devices raises these issues with renewed urgency.[15] It is time for the FTC to strongly reinforce to both consumers and device manufacturers the need to adopt strong security measures.

Consumers need to be aware of the risks posed by their IoT devices, and the FTC serves a critical role in offering that warning. It is the only federal agency with jurisdiction over consumer protection for broad areas of the economy.[16] As such, the FTC has an obligation to offer security warnings and to make information on changing passwords easily accessible to consumers.

Unfortunately, consumers do not always have the option of securing their own devices. Some device manufacturers have chosen to hard-wire in default passwords, leaving consumers helpless to remedy the problem. For these devices, only the manufacturer has the ability to update and secure the device to ensure it cannot be used in future attacks.[17] Additionally, most IoT devices are unable to protect themselves from botnets.[18] Manufacturers are often slow to patch vulnerabilities and many devices do not have the capacity to run antimalware solutions.

The FTC should immediately use all the tools at its disposal to ensure that manufacturers of IoT devices implement strong security measures to best protect consumers from cyberattacks. Future devices should not be sold in U.S. streams of commerce with deficient security mechanisms. Manufacturers should enable customers to change their passwords and in fact

---

[13] Federal Trade Commission, *Using IP Cameras Safely* (Aug. 2013) (online at www.consumer.ftc.gov/articles/0382-using-ip-cameras-safely).

[14] Federal Trade Commission, *Careful Connections: Building Security in the Internet of Things* (Jan. 2015) (online at www.ftc.gov/system/files/documents/plain-language/pdf0199-carefulconnections-buildingsecurityinternetofthings.pdf).

[15] *Friday's IoT-based DDoS Attack Has Security Experts Worried,* Computer World (Oct. 25, 2016).

[16] Federal Trade Commission, *About the FTC* (accessed Nov. 1, 2016) (online at www.ftc.gov/about-ftc).

[17] *Hacked Cameras, DVRs Powered Today's Massive Internet Outage*, Krebs on Security (Oct. 21, 2016).

[18] *What You Need to Know About the Imminent Threat of IoT Botnets,* Venture Beat (Oct. 1, 2016).

require customers to change default passwords during the set-up process. Additionally, manufacturers should patch vulnerabilities in IoT devices, so they cannot be exploited by botnets. These simple steps could significantly increase the security of IoT devices and mitigate future cyberattacks.

These efforts are just one part of a larger strategy to prevent and mitigate the effects of cyberattacks in the future. We look forward to working with you as partners to further increase security of IoT devices and ensure consumers are protected in this increasingly connected world. Thank you for your consideration of these requests.

Sincerely,

Frank Pallone, Jr.
Ranking Member
Committee on Energy and Commerce

Jan Schakowsky
Ranking Member
Subcommittee on Commerce,
Manufacturing, and Trade