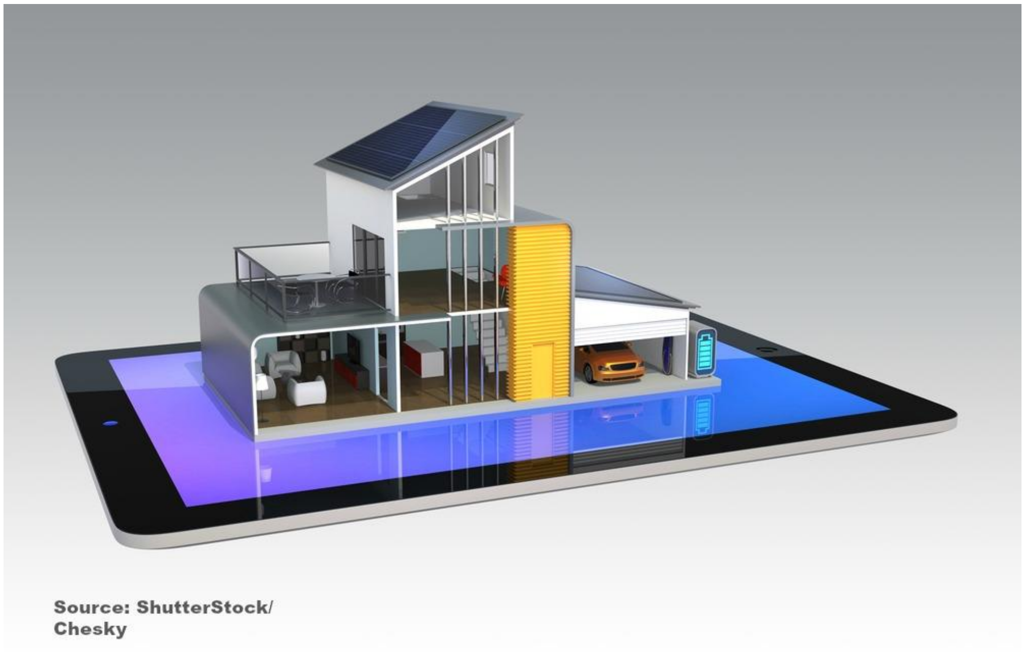
WHITE PAPER: WHAT THE HECK IS IOT AND WHY SHOULD HOMEOWNERS CARE?



Source: ShutterStock/ Chesky

2/13/2017

WHAT THE HECK IS IoT AND WHY SHOULD HOMEOWNERS CARE?

The increase of “smart” devices in our homes and offices leave us wide open to security breaches. The convenience of smart phones, thermostats, security cameras, baby monitors, door locks, medical devices, as well as other smart gadgets have lulled us into a false sense of security. When smart devices connect to, and communicate with, other global network “things” it is commonly referred to as the *Internet of Things (***IoT**).

In October 2016, the world saw how easily hackers were able to access common household devices, collect our data, and use that information to cause absolute mayhem on internet service. The target of that particular attack (a.k.a. **Mirai Botnet**) was a New Hampshire company known as DYN. Some of their clients (Netflix, Airbnb, and Twitter) had so many “hits” to their websites that it temporarily shut them down causing unwelcomed business disruption.

In this paper, we will address how easily hackers can sneak into your home to steal credentials and observe users. We will walk you through a rather simple, yet obscure, procedure to help you fend off plundering thieves who use your router as a backdoor to access your private information.

This paper will speak in plain English, offer no sales pitch, and present the facts. I hope you’ll find it useful.

Beverly Santini

Beverly Santini

The Philip Craig Group, LLC

Why all the hoopla?

Practically everyone in the developed world has at least one connected device in their home; often more than one. When you consider the sheer number of smart phones and tablets, it boggles the mind how device driven we have become.

With the increase of interconnected technology, we have opened our homes to more cyber dangers. Each device should be viewed as a target for villainous attacks. According to Jason Synder (Momentum CTO), "*we should be aware of what devices we're putting in our homes – connecting a device to a network changes things.*"

Cautions from other notable industry leaders are equally alarming:

- Unlike personal computers or servers, most IoT devices are not well protected – or even protected at all. Source: Igal Zeifman, Imperva Incapsula
- Right now, unfortunately, these devices are being sold by the millions, they're not secure, and bad things are going to happen. Source: Bruce Schneier
- Seventy-one percent of consumers fear their personal information may get stolen by using smart home products. In fact, consumers say they are more worried about this than they are about the cost of the technology. SOURCE: Chris Klein
- The smart home is woefully insecure due to users' failures to follow best practices. Source: Smart Home Security Report 2016 – Prplfoundation.org
- The IoT devices affected in the **Mirai** incidents were primarily home routers, network-enabled cameras, and digital video recorders (DVRs). Source: U.S. Computer Emergency Response Team (CERT)
- The time to address IoT security is right now. Source: U.S. Department of Homeland Security

You get the picture. Let's move on to how cyber thieves are able to procure your information.

Who are these scoundrels and how do they gain access?

Let's briefly look at the cast of characters.

First, there's the "**Cracker**." This bad guy is at the head of the invasion. The Cracker (or botmaster) is the one who actually breaks into your computer system, bypasses your woefully weak, factory-produced passwords, and takes over. Rarely does the general homeowner realize that the plundering has begun.

(c) Philip Craig Group/Matt Luckey

Botnets (essentially robots) are the armies of computers that have been compromised by the nefarious deeds of the Cracker. The bot specializes in finding vulnerable internet connected devices with similarly flimsy passwords and, voila, an army of bots (or zombies) is born. The entire army of zombies finds itself under the command and control of the **Bot Herder** for all sorts of menacing maneuvers.

How did you become an unwilling participant?

There are numerous ways the Cracker is able to walk through your online backdoor. Perhaps the greatest source of vulnerability is your home IoT devices. Items such as your home security system, wi-fi video doorbell, smart vanity mirrors, appliances, watches, home theaters are susceptible to online security breaches.

Connected devices are, by nature, insecure

We're all eager to use anything that makes our lives easier. Manufacturers are anxious to pump their products into our hands as fast as they can. That's just good business.

What's not good business is their failure to prioritize security measures within their merchandise.

Computer routers and modems fall into this category. The designers often apply the same password to their particular branded product and those easily fail the "strong" password benchmark. For example, your router's factory installed password, along with the thousands of other routers sold by the same manufacturer, might be "router 123456" or something equally as dreadful. These really bad, and easy to guess, passwords can be quickly hacked by lurking Crackers.

> **"IoT devices, on average, get hacked within 6 minutes of going online due to Users who do not change their default passwords."**
>
> **Ryan Davis, TechForge Media**

So now that the Crackers are in command and control of your computer, they can use your devices to assist them in their sinister undertakings. This may, or may not, include stealing your personal financial information which can be even more devastating.

What can you do?

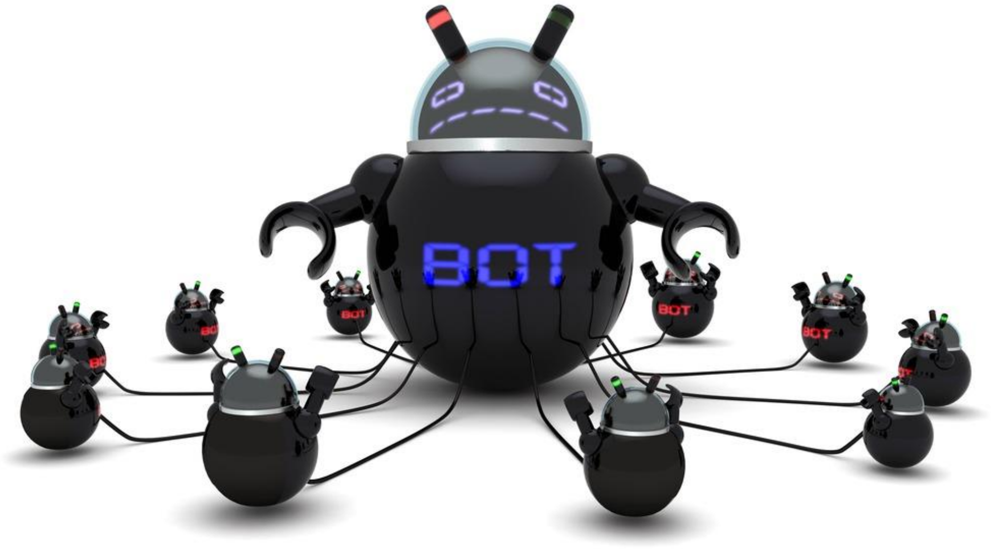
There is nothing "hack free" at this point. Until manufacturers give more attention to securing their products, we, the consumers, are at the Cracker's mercy.

We can, however, place a few strategic mines in the pirates' pathway.

1. Change the crappy passwords on your router. It's not that difficult. If, however, you're a self-described technophobe, call someone to come in to do it for you. Yes, it's that important.

2. Make sure you update the software when notified. I know that most of us ignore these irksome announcements but it is an essential element in your security game plan.
3. Add a firewall to your system and make sure it remains closed!

Implementing these strategies will help reduce your chances of being inducted into the botnet army.



Source: ShutterStock/Gunnar Assmy

What’s next?

We hope this White Paper has been enlightening. There are many advantages to living in a “connected” world and, as we move forward, our lives will be increasingly impacted by the Internet of Things. We now share in the responsibility of making it a little safer.

To help in that endeavor, we have included instructions on how to change the default password on your router. Again, it serves as a precautionary measure to thwart the hacktivists from gaining access to your computer’s treasure trove of information. Do spend a few moments in reviewing the Appendix in order to take your first step in fortifying your home’s online security.

We welcome your comments and look forward to bringing you more in-depth articles surrounding the Internet of Things.

Beverly Santini

Beverly Santini

President/The Philip Craig Group

APPENDIX

HOW TO CHANGE ROUTER DEFAULT PASSWORD

STEP	ACTION
1	Determine Router Brand/Model (Look on Router for information)
2	Identify the IP address for your router brand & model ***NOTE:*** If the router is brand new, this information will be in the instructions. If you only know Brand/Model information, you can look at these two websites to get IP Address, User Name & password. www.routeripaddress.com and/or www.routerpasswords.com
3	Open Browser
4	Type in Router IP Address
5	Depending on Brand/Model, a Pop-Up Window should appear asking for default User Name & password.
6	Follow prompts to complete password change
7	Save changes and keep your password handy for future use

NOTE: Each Brand/Model differs in process but generally each has a Wireless Security tab.