* Block against personal hacks
* **Ryall and Abbruzzese 2016; An attacker gets into your device by** using a piece of computer code that searches for any **internet-connected devices that have default settings.**This means if you **Haven't updated your login and password from admin and admin, you are probably being targeted.** The malware code scans the internet looking for these devices, which it can then enter and turn into zombies later used to launch an attack on a particular target. But how do you stop this happening? With the average person becoming more and more connected to the internet and introducing more and more devices into their network, being security aware is more important than ever.
* If the one thing standing between the implementation of Iot is the difference between people who are preoccupied and trivialize changing their password, than our opponents are negating low magnitude arguments.
* http://mashable.com/2016/10/21/protect-home-devices-iot-hacks/#OFN2DU.MpSq4
* Block against likelihood of Ddos
* **Barker 16** The number of **DDoS attacks fell more than 40 percent to 97,700 attacks in the second quarter of 2016** according to the latest threat report from **DDoS security service Nexusguard.**
* **The report reveals there was a sharp dip in distributed reflection denial of service** (DrDoS) **attacks, with DNS-based attacks falling 97 percent compared to the previous quarter.** However, recent DDoS attacks on cybercrime journalist Brian Krebs and OVH, a French internet hosting provider, broke records for speed and size.
* Nexusguard researchers put the drop in reflection attacks and the success of these massive attacks to hackers favoring Mirai-style botnets of hijacked connected devices, demonstrating the power the Internet of Things has to threaten major organizations. With increasing pressure on hosting and internet service providers to fend off fierce attacks against customers, Nexusguard analysts advise organizations to ensure they use signature-based detection to quickly identify and thwart botnets.
* As we can see these attacks are decreasing in likelihood, the devices are more widely available, and groups of people are unwilling to challenge the software new protection that is becoming more widely available.
* <http://betanews.com/2016/11/01/ddos-speed-size-increase/>
* **DDos prevention software**
* **Paap 2015; Common DDoS protection deployments use a flow analytics device, which reacts to the discovered incident by redirecting the victim’s traffic to a mitigation device and telling it what action to take. This method scales well for gathering traffic to be analyzed, and the reactive model only redirects potentially bad traffic, which allows for some bandwidth oversubscription.** But this is risky business as the mean time to mitigate can run into minutes.
* As we can see, Ddos prevention software is available In the status quo, and it gives information to the respective company so that they can prevent themselves in the future, by implementing IoT you are cross applying the destruction of Ddos attacks and businesses can prevent future attacks.
* <http://www.networkworld.com/article/2905115/network-security/the-best-way-to-stop-ddos-attacks.html>

Block to how to prevent Ddos, goes with number one

The Internet of Things is going to change the way we live in a big way. Whether it's in the home, in the car or at the office, more and more Internet-enabled devices or “things" will come online and perform tasks such as regulating the temperature in your house, unlocking your doors, monitoring your car's performance, adjusting your lights, slow cooking a meal and more. All that you need to take advantage of these new capabilities is a good home Wi-Fi network and a smartphone or tablet.

However, with all this new technology and functionality come new vulnerabilities, including increased risk of security breaches that can result in your data falling into the hands of hackers. So what do you need to do to protect yourself, your data and your devices from these wrongful people? First, you need to protect the networks and devices that are interacting with your new connected “things." Here are some tips we have found that will be helpful in securing your home, car and wearables:

How to secure your connected home.

Since the key components for a connected home are your smartphone/tablet and your Wi-Fi network, these are the first things you need to make sure are well protected.

Here are some tips we got from Symantec on how to secure your home network:

* **Change the default username** and administrative passwords on all wireless equipment and devices that connect to your network. Make sure those passwords are strong and secure.
* **Enable Wi-Fi Protected Access (WPA)** on your router. WPA is a security protocol that encrypts the data sent on your network so that it can't be intercepted by outsiders. Some routers might also -- or in some cases only -- support an older protocol called WEP (Wireless Encryption Protocol), but that's not as secure.
* **Make sure the hardware firewall in your router** and software firewall on your computer are enabled and working.
* Since experts say that the free security software that comes with Windows computers offers weak protection, **add an extra layer** of security to your computers by installing and using strong third-party security software such as Norton Security. Your wireless network might be secure from intruders, but your computer is not secure from the various types of malware that can be transmitted via the Internet. Everything is connected.

Next you need to make sure you secure your smartphone/tablet. Once again, here are some tips from [Symantec](http://www.tkqlhce.com/click-7718664-10563533-1411420025000" \t "_blank) on how best to do that:

* **Use a screen lock password** on your phone to keep others from accessing your phone. Make sure your device auto-locks when not in use. Be sure to have an option or a security app that can remotely wipe the data from your phone in the event that it is lost or stolen.
* **Pay attention to app privacy** policies. The privacy policy should inform you of what information the app intends to access on your phone, what data it is collecting, and what it intends to do with that information. Avoid any app that seems to be particularly intrusive, collecting data that seems to be unnecessary for what it does.
* **Be sure to perform regular software updates** on all apps and your phone's operating system. This will patch possible security vulnerabilities that can give malware and cybercriminals access to your phone.

How to secure your connected car.

The two biggest concerns with a connected car are the vehicle's computer system and the data it collects and stores. Today, some new cars have elaborate computer systems that allow access to more than just your entertainment system and hands-free calling. Manufacturers are teaming up with computer developers to offer all-inclusive computerized interfaces for vehicles. Right now, the services and applications used are delivered in two ways: using smartphones and tablets connected to the car via Bluetooth or using a computer system that's built into the car itself with its own set of wireless connections to the outside world. Did you know that the computer systems in some cars can send GPS tracking out to report traffic jams and find faster routes?

According to [Symantec](http://www.tkqlhce.com/click-7718664-10563533-1411420025000" \t "_blank), security breaches via the car's computer system can happen in two ways: via the car's built in wireless interfaces or through physical access to the car itself. Remotely, hackers can use virtually any wireless interface in the car -- Bluetooth, short range Wi-Fi, GPS, cell phone, etc. -- to gain access to the car's computer and systems. [A study published by University of California, San Diego](http://cse.ucsd.edu/node/736" \t "_blank), reports that someone inside the car can also gain access to the vehicle's computer via the stereo system or the car-alarm system. You need to make sure that all of these systems and devices are protected.

Here are some tips we found on how best to prevent hackers from gaining access to your connected car's computer system, the data it collects and stores, or the smartphone/tablet you bring along for the ride:

* Secure your smartphone, as this is an easier target for hackers.
* Within any app, via the vehicle itself or the app on your phone, be sure to change the default admin username and password.
* Update software as soon as it is available. This patches vulnerable security holes.
* Don't reuse the same passwords across apps.
* Only visit certified repair centers. Dishonest shops can steal data, inject malware and trigger false repair alerts.
* If you want to install aftermarket parts, check with your car dealer first to make sure they are safe.
* Turn off your phone's GPS when not using GPS services. This makes it harder to constantly track your location (this reduces the drain on your phone's battery, too!).
* Be careful of what you share on social media. If you must allow apps access to your Facebook profile or Twitter account, try to be a bit more aware of what you upload to them. Is there really any need to include your most personal information about your car and where you are on social networking sites?

Summary

The Internet of Things is going to change the way we live and work. Billions of new devices will be coming online to provide a tremendous amount of convenience for everyone, but they will also bring with them a host of new security concerns. For now, implementing the safeguards listed above will help protect you and your data. While the future is still unknown, we are confident that any new technology that comes to market will give rise to new security solutions to stay ahead -- or at least keep up -- with the bad guys. So be sure to stay in contact with your security provider for new software updates.

http://www.gearbrain.com/how-do-you-protect-your-privacy-and-data-in-an-internet-of-things-worl-1622024544.html