

Security Awareness News

the security awareness newsletter for security aware people

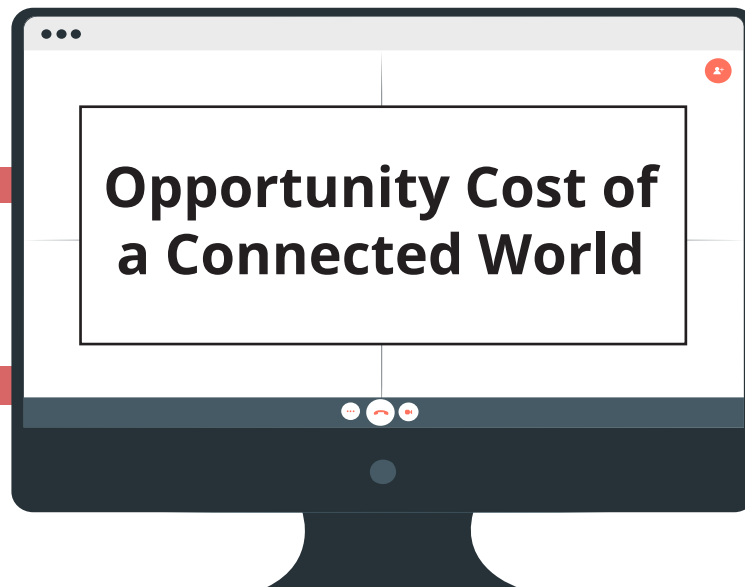
The Internet of Hackable Things

Opportunity Cost of a Connected World

Securing Your Smart Devices

Artificial Intelligence and the Future of Security





The Internet of Things, or IoT, refers to the broad range of internet-connected devices that offer many different services and functionality. From consumer products, like digital assistants and remotely accessible security cameras, to smart hospitals and manufacturing plants, the potential advantages of the IoT are nearly limitless. But there's also an opportunity cost associated with this connected world.

Opportunity cost is an economic principle that simply means if you choose Option A (whatever that may be), you are effectively giving up the opportunity to choose Option B. The concept of work/life balance is a great example. The more someone works, the more money they'll have. But that comes at the expense of having less time. So time is the opportunity cost.

The opportunity cost of IoT is similar: It can improve the quality of life at the cost of risking privacy, security, and even physical safety. Let's examine all three of those risks.

PRIVACY

Smart devices collect a significant amount of data from users and their environments. If not properly secured, that data could be accessed by unauthorized parties for malicious purposes such as identity theft – a type of fraud where someone uses stolen personal information to open accounts in the victim's name.

SECURITY

Many devices lack adequate security features, which makes them highly susceptible to cyberattacks. They also often ship with default passwords that some consumers fail to update, which makes those devices especially vulnerable.

SAFETY

Imagine a criminal discovered a vulnerability of an internet-connected machine at a factory that allowed them to take control of the machine. They could exploit that vulnerability to cause physical damage and put the physical safety of workers at risk.

Clearly, IoT unlocks an amazing world of potential, but it also unlocks a world of concerns. The question then becomes: How can we take advantage of that potential while mitigating some of those concerns? At work, the answer is simple: Follow policies, especially where connecting personal devices to an organization's network is concerned.

On the next page, we'll cover a few tips and tricks for securing your personal devices and data. Just keep opportunity cost in mind when you add smart gadgets to your life!

Securing Your Smart Devices

Isn't it annoying when a webpage won't load? Imagine how much more annoying it would be if every website you visit on a daily basis suddenly stopped working. That's what happens during major DDoS attacks that target internet servers.

What Is DDoS?

DDoS stands for distributed denial-of-service. It's a cyberattack that floods servers with more information than they can handle, causing them to crash. This can knock services offline for thousands of organizations and cause internet outages for millions of people.






What's a Botnet?

When multiple internet-connected devices get infected with malicious software, cybercriminals can take control of those devices and form an army of attackers known as a botnet. The term botnet is short for "robot network", and it's how DDoS attacks are launched.

What Can Be Done To Prevent DDoS Attacks?

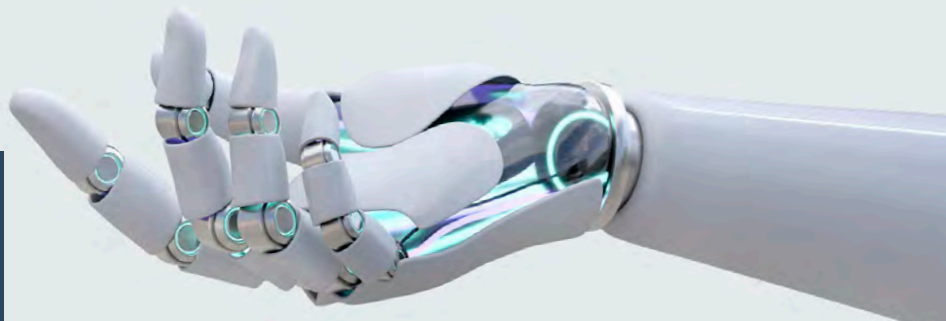
Organizations that use IoT must take appropriate measures to secure it, which can include implementing strong authentication and encryption, monitoring network traffic for unusual activity, and keeping devices updated.

Additionally, consumers can also do their part. Here are a few ways to protect any smart devices you might own:

-  **Do some research.** The best way to combat security concerns is by researching products and only purchasing the ones that offer robust security controls or privacy settings.
-  **Update default passwords immediately.** Many devices ship with default login credentials that are public knowledge. Change them as soon as you power up the device.
-  **Enable automatic updates.** Outdated devices and software could have security vulnerabilities. Wherever possible, ensure your internet-connected things are always on the latest updates.
-  **Disable unnecessary features.** Take a "less is more" approach to security and disable any features you don't need or won't use. This can help reduce personal data collection.
-  **Occasionally review privacy settings.** While updates are vital, developers sometimes push new features with updates that might change various settings. Make a habit of occasionally reviewing privacy settings to ensure they're set to your preferences.

Remember: Smart connections usually equal data collection. So while technology can be amazing, it needs a little hands-on effort to protect personal information and prevent cyberattacks like DDoS.

Artificial Intelligence and the Future of Security



Artificial intelligence (AI) refers to the simulation of human intelligence in machines that are programmed to think and learn like humans. AI can be divided into several different types, including:

- **Rule-based systems**, which follow a set of predetermined rules to reach a conclusion
- **Expert systems**, which use a knowledge base to make decisions
- **Neural networks**, which are modeled after the human brain and can learn from data
- **Natural language processing**, which enables machines to understand and interpret human language

AI technology has been developed in various areas such as image recognition, self-driving cars, personal assistants, and so on. There are several security concerns regarding AI technology. Here are a couple of examples:

Data poisoning: In some cases, attackers may try to inject malicious data into the training dataset to “poison” the model and cause it to make incorrect decisions.

Physical safety: Some AI applications, such as self-driving cars or industrial robots, may pose physical safety risks if they malfunction or are compromised by an attacker.

By the way, everything you’ve read on this page (up until now) was not written by a human, but by an AI chatbot. It was simply asked to define artificial intelligence and explain the related security concerns. If you wanted to, you could ask that same bot to write poetry about cats, explain quantum physics, or basically anything else you can think of. The chatbot is a basic example that barely captures AI’s capabilities.

As it evolves, AI technology will become even more advanced with abilities we never thought possible of machines. This, of course, ushers in all sorts of interesting conversations regarding human intelligence vs. machine intelligence, and what might happen if the latter surpasses the former.

Those conversations make this quote from the 1993 movie *Jurassic Park* eerily relevant: “Your scientists were so preoccupied with whether they could, they didn’t stop to think if they should.”

Nonetheless, AI is an active part of our lives. And it’s not hard to imagine cybercriminals leveraging AI to carry out attacks in the near future. As an example, AI models could learn about a real person and then use bots to mimic their actions and language. This would allow criminals to create advanced phishing campaigns that target specific people at a much more effective rate than any human could.

It’s also possible AI will be used to circumvent attacks from criminal hackers. But even as those technologies become more of a reality, advancements in cyberdefenses will always lag behind advancements in cyberattacks.

Therefore, the future of security is the same as the present: humans, not machines. It will take a human effort to identify modern attacks and prevent them from finding success. So stay alert, stay informed, and remember that the last line of defense was, is, and will continue to be people like you.