SecurityAwarenessNews

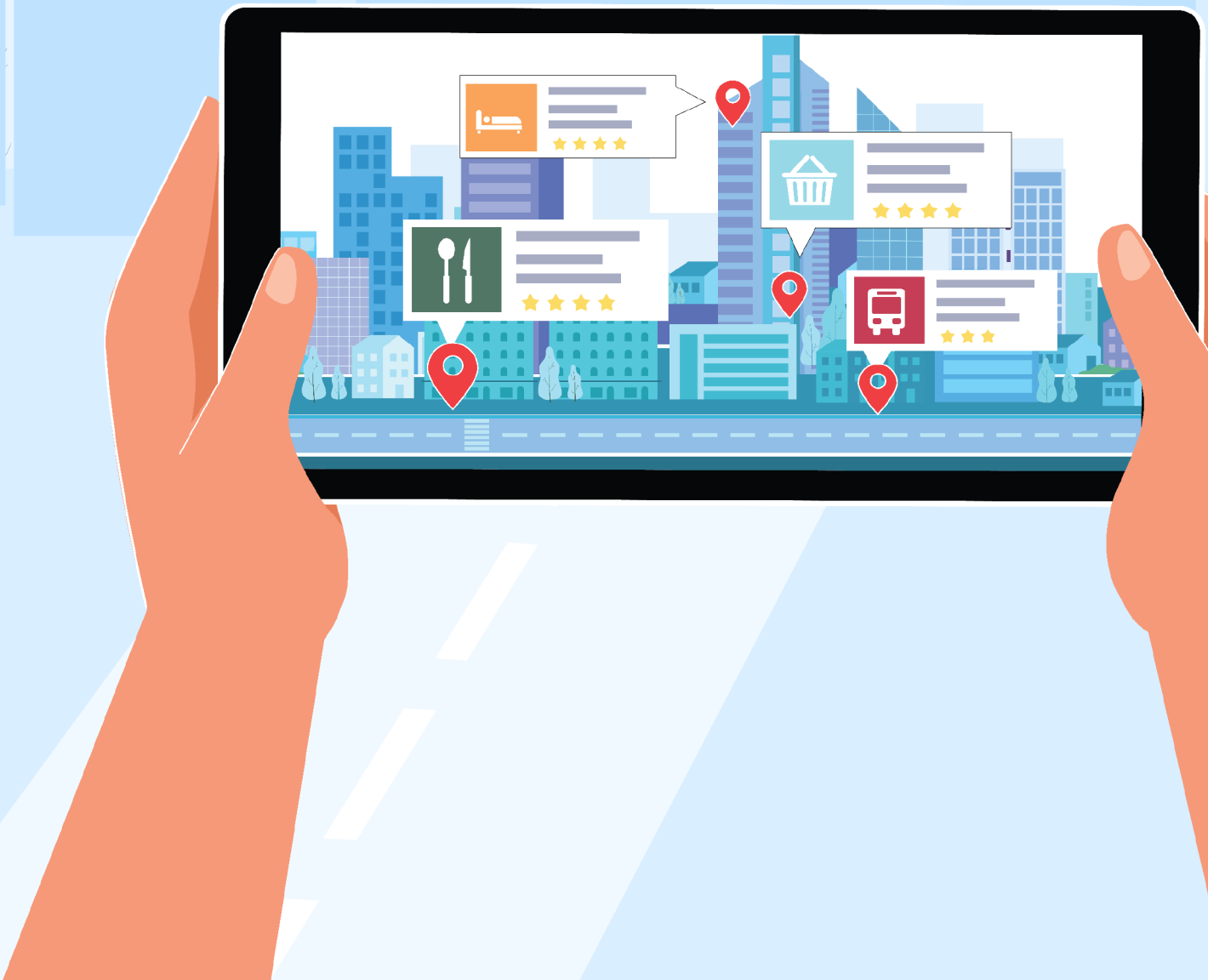
the security awareness newsletter for security aware people

Smart Security for a Smart World

The Threat of IoT

Securing Your Smart Home

The Future of Security



The Threat of IoT

Welcome to the Internet of Things (IoT): a world where your refrigerator can play YouTube videos and your thermostat can help reduce energy costs by adapting to your environment. For anyone that's unfamiliar with the IoT, which is simply a network of connected smart devices, let's take a quick tour of a few common applications:

SMART APPLIANCES:
coffeemakers, refrigerators, ovens, and nearly every common household appliance can now connect to your network and offer a variety of handy features.

SMART WEARABLES:
want to track your sleep patterns and general health data? That's never been easier thanks to things like smart watches, armbands, and even jewelry.

SMART LIGHTS:
set the mood with light bulbs that allow you to control their brightness, color, and on/off schedules with the click of a button.

SMART HOME SECURITY:
internet-connected doorbells and cameras offer a great solution for people who want to monitor their homes from anywhere in the world.

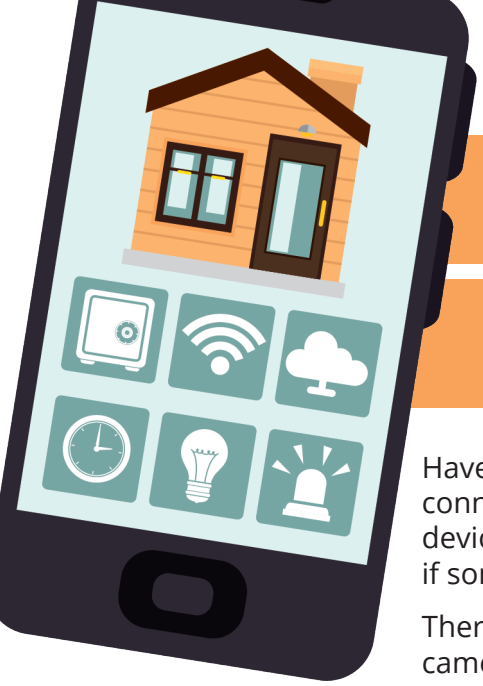
SMART HEALTHCARE:
the Internet of Medical Things (IoMT) can monitor a patient and collect data that helps healthcare professionals make better decisions about treatments.

SMART FACTORIES:
known as Industry 4.0, smart factories utilize the IoT to improve efficiency and accuracy of production via automated processes.

SMART HUMANS?
We sure hope so. The notable downside of smart things is the amount of data they collect and the access they require. That combination breeds obvious privacy concerns, which are exacerbated by the fact that many of these devices have few built-in security features. As such, maintaining privacy once again requires smart, security-aware people.

On the next page, we're going to dive into how you can utilize the IoT at home while also keeping your data safe.

Here at work, remember to always follow policy regarding what personal devices are allowed to connect to networks and work-related accounts. If you notice a work device acting strangely, report it immediately. Have questions? Please ask!



Securing Your Smart Home

Have you heard of Amazon Sidewalk? It's a new feature that shares the internet connection of your Amazon smart devices (Echo, Ring, etc.) with your neighbors' devices. The idea is to create neighborhoods that always remain connected, even if someone's internet goes down.

There are plenty of advantages to this concept. If you have a home security camera, for example, and you lose internet access, it can automatically connect to your neighbor's network and remain operational.

But the announcement of Amazon Sidewalk immediately caused privacy advocates to sound the alarm. It doesn't help that Amazon devices are automatically opted into the service, rather than consumers electing to opt in—a function that leaves many questioning Amazon's intentions.

We use this example to illustrate how the IoT blends an uncomfortable mix of convenience with concerns of privacy. Could Sidewalk end up being a highly beneficial feature that improves our lives? Sure! Could it also result in potential security issues? Absolutely. It's another situation where we as consumers need to stay aware of what big companies are doing with the products and services we use.

With that in mind, let's quickly review a few ways you can take advantage of the convenience offered by IoT while still maintaining privacy and security.

1. **Do your research.** Developers usually focus on smart features and view security as an afterthought. Consumers need to prioritize security as a forethought and favor devices that offer robust security controls.
2. **Use strong passwords.** Some new devices may ship with default login credentials. These need to be updated immediately to strong, unique passwords wherever possible.
3. **Stay updated.** For any devices that offer it, enable automatic updates. Outdated software and firmware can lead to security vulnerabilities.
4. **Remain proactive**. The Amazon Sidewalk example demonstrates how important it is for consumers to proactively address security. Occasionally review security settings of all devices.
5. **Avoid the IoT.** While the IoT offers great convenience, sometimes it's best to turn off smart functions and avoid the data collection often associated with these devices.

What is DDOS?

DDoS stands for distributed denial-of-service. It's a cyberattack that uses thousands of hacked smart devices to flood internet servers with more traffic than they can handle, causing them to crash and knocking major services offline.

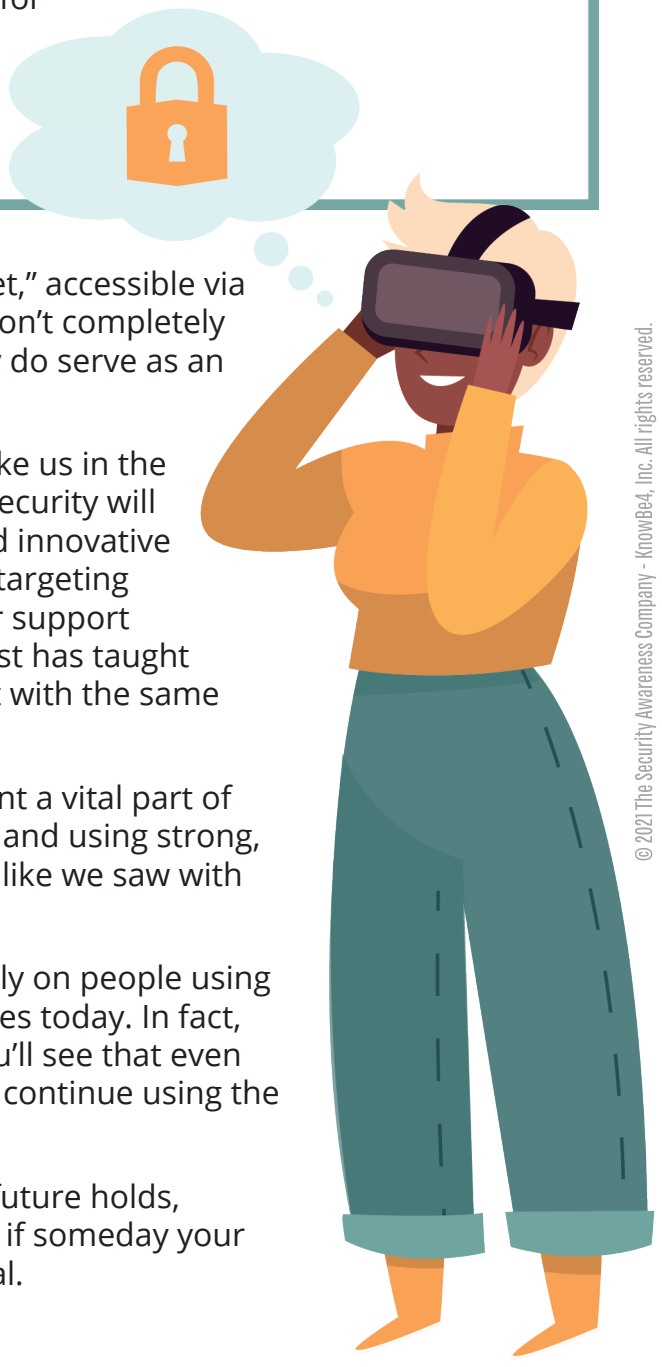
If you want to learn more about the dangers of DDoS, look up the Mirai botnet (the name given to armies of hacked smart devices) and read about how it has impacted hundreds of thousands of people. DDoS is one of the main reasons why security experts warn that the IoT represents a major and ongoing security concern.

The Future of Security

Imagine a future where traditional workplaces no longer exist. No more buildings full of computers and conference rooms. No more video calls using webcams. Instead, you join meetings as an avatar (your online character) and collaborate with your co-workers in a fully immersive, virtual environment from the comfort of your home.

After work, you quickly switch avatars and attend a live concert presented in 360-degree audio and video that allows you to enjoy the show from multiple viewpoints. You can even buy digital clothes and other forms of concert swag for your avatar while interacting with real people from all over the world.

Both of these scenarios exist in a digital space known as the metaverse—a virtual domain that hosts alternatives to real life events such as gaming, live sports, education, social gatherings, and others.



Currently, the metaverse is emerging as the "new internet," accessible via virtual reality headsets. The concepts described above won't completely replace real-life events anytime soon (we hope), but they do serve as an example of what life may look like in the near future.

And while it's difficult to predict where technology will take us in the coming years, we can confidently say that the future of security will face new challenges. Cybercriminals are never far behind innovative trends. To see this in action, look up how scammers are targeting OpenSea—a digital marketplace—by posing as customer support representatives. New technology; old scam. But if the past has taught us anything, it's that security challenges will likely be met with the same solutions we use today.

For example, always following policy will forever represent a vital part of security. As will immediately reporting security incidents and using strong, unique passwords (even if new alternatives come online like we saw with fingerprint scanners and facial recognition).

The key takeaway is this: security in the future will still rely on people using common sense and making smart decisions, just as it does today. In fact, if you look back at all of the scams of the last decade, you'll see that even though technology has greatly improved, cybercriminals continue using the same old tricks (namely phishing).

So, as we transition into new realities and whatever the future holds, remember to stay alert and think before you click—even if someday your mouse is virtual, and your workspace is completely digital.