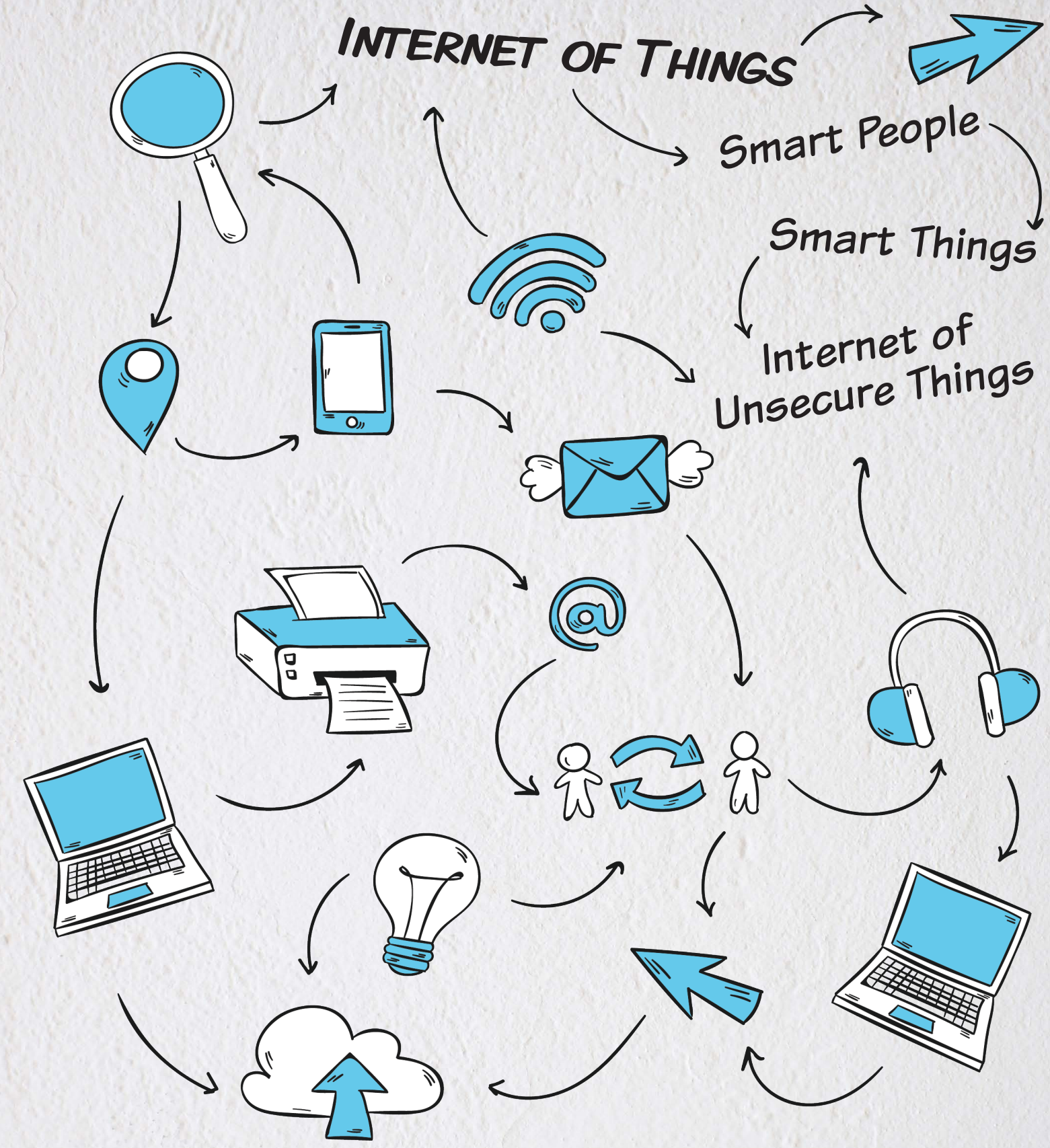
SecurityAwarenessNews

the security awareness newsletter for security aware people



Smart Things

The Internet of Things (IoT) provides unprecedented interconnectivity between devices and humans that improves everyday life.

Smart Homes

Lights, alarm systems, security cameras, thermostats, digital assistants, appliances, and a multitude of other connected devices have revolutionized our living quarters while creating "greener" neighborhoods.

Smart Factories

Known as Industry 4.0, smart factories utilize metrics and data of computer-controlled equipment to increase efficiency and safety of production.

Smart Cities

More than just free WiFi on every corner, smart cities use real-time data to reduce traffic, save energy, improve public safety, and monitor critical infrastructure like water supply and power grids.

Smart Cars

Driving has never been easier thanks to automatic parking features, adaptive cruise control, lane assist, real-time traffic analysis, and optimized fuel consumption. Some cars are even self-driving now!

Smart Healthcare

From fitness trackers to smart hospitals, the IoT improves human health by collecting data that helps doctors quickly identify concerns, while also lowering operational costs.

The IoT unlocks a world of potential, but it also unlocks a world of security concerns, considering the amount of data being collected, transferred, and stored. Here at work, always follow our organization's policies, and stay alert for scams, both in the real world and on the internet. At home, limit the amount of data you share, and research products before adding them to your life.

Smart Humans

- Create strong, unique passwords for all accounts and devices that are easy to remember but hard to guess.
- Use situational awareness when traveling or working remotely.
- Stay alert for social engineering attacks at work, home, and on the go.
- Hover over links to reveal the full URL, and click with caution.
- Keep devices up to date, and enable automatic updates where available.
- Follow organizational policies, and ask questions when unsure of something.
- Report all security incidents immediately.

Smart Humans vs. Smart Things

Regardless of how technology improves, the world will always need smart humans to battle cybercrime. From fitness trackers to home security systems, and a seemingly endless market of smart devices, everyday functions now generate more data than ever. In fact, over 90% of the world's data was generated in the last two years. As such, when adding smart things to your personal life, consider the ramifications. If possible, enable the maximum security settings available, and disable any features you don't use. Here at work, never connect a smart device to our network unless it has been approved by management.

Internet of Unsecure Things

How Cybercriminals Use the IoT Against Us

While the Internet of Things has great potential to improve our lives, it also poses major security risks. Here are a few examples of IoT gone wrong:

Botnets: When multiple smart devices get infected with malware, cybercriminals can turn them into botnets—an army of compromised devices that attack networks and knock services offline.

Espionage: Imagine if a cybercriminal hijacked the camera and microphone of every internet-connected device at a government building.

Physical Destruction: As more and more smart factories, smart cities, and smart cars come online, the concerns of physical destruction grow. For example, a hacked device could overrule safety settings of machinery, causing them to catastrophically fail or explode.

Mortal Danger: Physical destruction could cause loss of life, and so could compromised healthcare devices such as implantable cardiac devices. Here's a real-world example: CNN Business article - FDA confirms that St. Jude's cardiac devices can be hacked.

What makes the IoT so vulnerable?

The fierce competition among manufacturers of smart devices tends to favor marketability over security. As a result, products enter the marketplace with inadequate security settings, often with no option to update potential flaws. Making matters worse, some consumers fail to change default credentials or forget to institute maximum privacy options.

Securing Smart Devices

- **Update default passwords immediately.** Many devices come with default login credentials that are public knowledge. Change them as soon as you power up the device.
- **Enable automatic updates if the option exists.** Most smartphones, apps, gaming systems, and other devices allow automatic updates, which provide immediate security patches and upgrades.
- **Maximize privacy settings.** Some settings may allow manufacturers to collect your data by default. Edit these settings to the minimum necessary for the device to properly function.
- **Disable unnecessary features.** Take a "less is more" approach to security, and disable any features you don't need or won't use.
- **Do some research.** The best way to secure smart devices is by researching products and only purchasing those that were built with security in mind.

Here at work, always follow our organization's policies.
If you have any questions or need more information, please don't hesitate to ask!