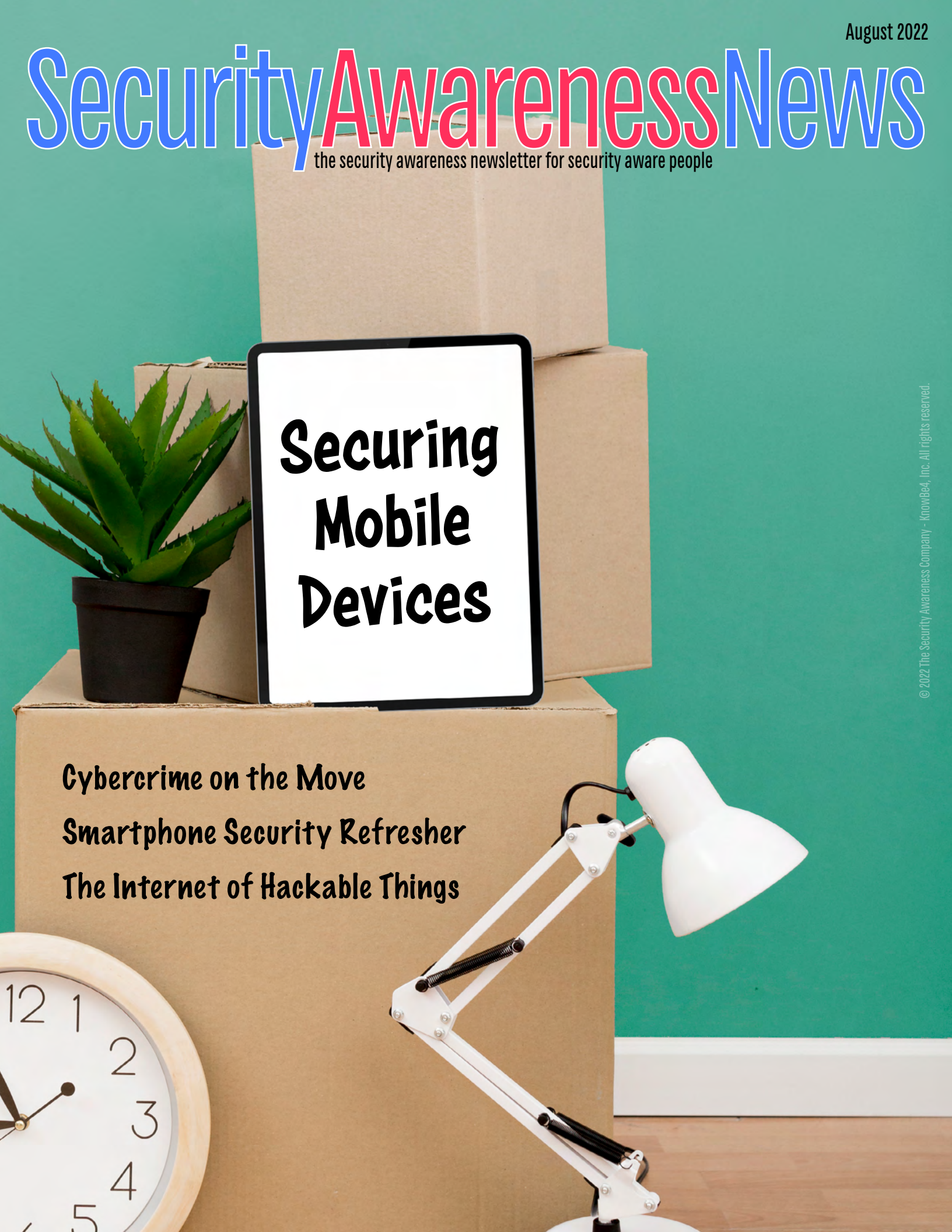
August 2022

SecurityAwarenessNews

the security awareness newsletter for security aware people



Cybercrime on the Move

Smartphone Security Refresher

The Internet of Hackable Things

Cybercrime on the Move

With billions of active mobile devices connecting the world, it's no surprise that cybercriminals have shifted a large portion of their focus to this attack vector. Let's review a few common ways they utilize the mobile market to spread malware, steal data, and launch other cyberattacks.

Smishing

Smishing attacks utilize traditional phishing techniques and deliver them to you via text message. A common example is a text that claims your bank account has been compromised. It instructs you to immediately click the included link and update your username and password.

Avoid it: Never click on links in random text messages, especially if they include threatening language.

Malicious Applications

Popular app stores are notoriously targeted with malicious applications that steal data and spread malware. Even though the large app stores have strenuous procedures in place to eliminate criminals, they still manage to slip through.

Avoid it: Do a little bit of research, and ensure that the apps you intend to install are trustworthy.

USB Charging Cables

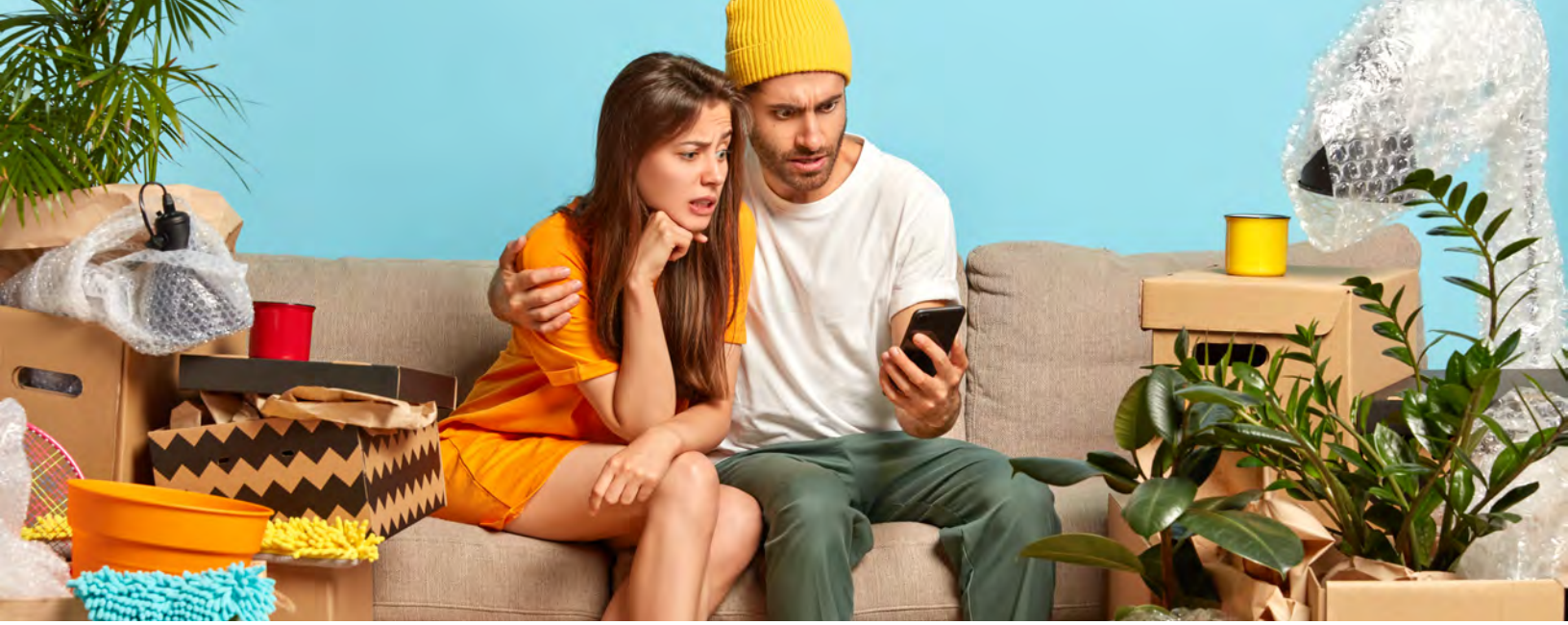
Did you know that common USB charging cables can be used to distribute malware? This means that attackers can leave malicious cables in public areas. If someone plugs that cable into their phone, the attacker can then install malware on the victim's device.

Avoid it: Only use the charging cables that you own. Avoid public charging stations.

DDoS Attacks

Short for distributed denial-of-service, DDoS attacks use malware-infected smart devices (security cameras, smart appliances, etc.) to flood internet servers with more traffic than they can handle. This causes the servers to crash, which can knock services offline for hundreds of thousands of people.

Avoid it: Protect every smart device with a strong, unique password.



Smartphone Security Refresher

One of the biggest challenges for organizations worldwide is finding a balance between security and allowing employees to use personal devices for work-related tasks. Of course, this challenge is not something the majority of employees need to think about. But we can all help by understanding and always following organizational mobile policies.

8 Tips for Smartphone Security

1 **Lock it Up**
a device with a strong password or PIN. Lock it immediately when not in use.

2 **Keep it Updated**
For personal phones, consider enabling automatic updates so you never miss a vital security patch.

3 **Keep it Clean**
Occasionally review and remove unused applications to avoid concerns related to data privacy.

4 **Be Selective**
Research applications before installing and only download software from trusted vendors or developers.

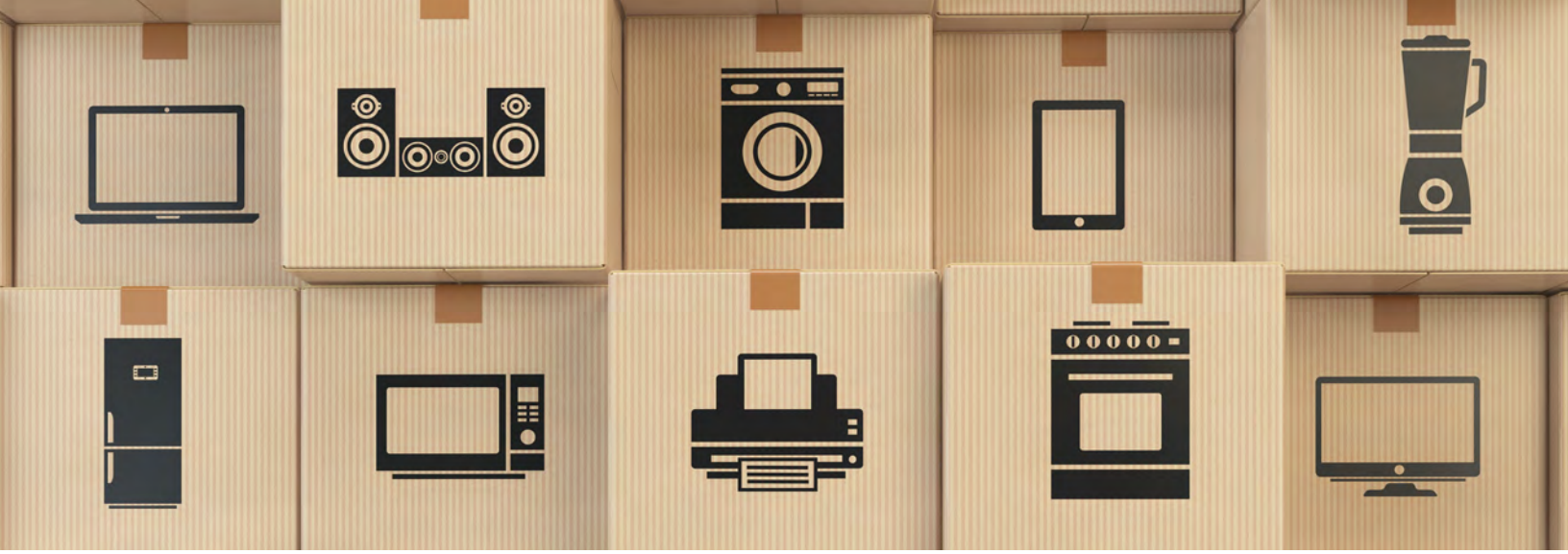
5 **Limit Permissions**
Where possible, only allow the permissions that are necessary for an app to function.

6 **Store it Securely**
When traveling or working remotely, always store your device where it can't be easily stolen.

7 **Enable "Find My Device" Services**
This feature helps locate a lost smartphone, and/or removes all personal data from it via a second device.

8 **Think Before You Click**
Avoid clicking on links that are sent to you randomly or from unknown contacts.

Remember: Smartphones allow us to access almost anything from anywhere. That invaluable convenience also exposes us to a long list of security concerns. Be sure to give your smart devices the same security care that you would a traditional computer.



The Internet of Hackable Things

The Internet of Things (IoT) provides unprecedented interconnectivity between devices and humans. From smart appliances to smart cars and even smart cities, the IoT unlocks a world of potential that can improve our lives.

It also unlocks a world of risks. Many smart devices are built to favor functionality over security. As a result, products sometimes enter the marketplace with inadequate security and privacy settings. Considering the amount of personal information many devices collect, the concerns surrounding the IoT are more than justified. This leads us to a simple fact: we will always need smart humans to mitigate the risks associated with smart things.

Securing the IoT

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. As a reminder, outdated devices pose security risks. 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.

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.

Unplug it. Similar to disabling unnecessary features, it's also best to disconnect devices that aren't routinely used and limit their access to your network.

Remember: There will always be a tradeoff between data privacy and enjoying the convenience of smart devices. By design, the IoT needs to collect information in order to function. That information is stored on an internet server somewhere, and you can bet that cybercriminals are currently looking for a way to access it. As such, when adding smart things to your personal life, consider the ramifications. Here at work, never connect a smart device to our network unless it has been explicitly approved.