Safety FOCUSED

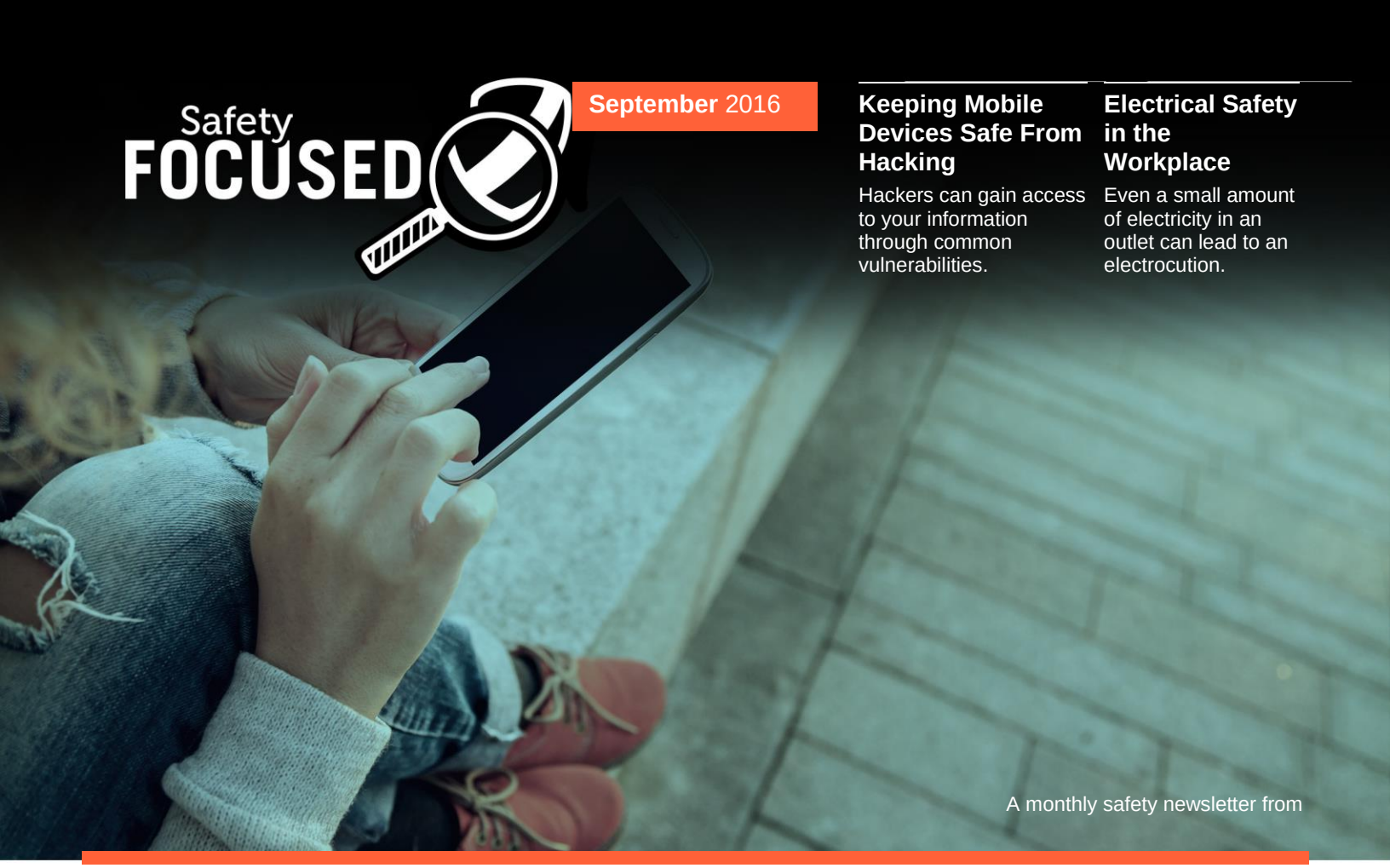
**September** 2016

**Keeping Mobile Devices Safe From Hacking**

Hackers can gain access to your information through common vulnerabilities.

**Electrical Safety in the Workplace**

Even a small amount of electricity in an outlet can lead to an electrocution.



A monthly safety newsletter from

# Keeping Mobile Devices Safe From Hacking

As smartphones and other mobile devices have advanced and added conveniences for users, they have also become more susceptible to cyber attacks. And, if you don't take steps to protect the personal or work information on your devices, you could be exposed to considerable risks.

A hacker can attack a smartphone or other mobile device without the owner's knowledge and gain access to his or her messages, contacts, emails and even his or her location, based on GPS data. Additionally, individual cyber attacks are beginning to exponentially increase in frequency. Although a few years ago hackers mainly targeted retailers and health care organizations, they now see individuals as a key target.

To protect the information on your devices, you need to know the main vulnerabilities that hackers can exploit to their advantage:

- **Malicious apps:** Many apps ask for more access to your device than is required. When you download an app, make sure to check how much access it has, and that the app has been made by a reputable developer. Additionally, always download an app from your device manufacturer's official store. Apps downloaded from a website or mobile link are much more likely to contain malicious code.
- **Unsecured networks:** Hackers can use public Wi-Fi and other unsecured networks to see all of your internet usage. Avoid using public networks when possible, and disconnect from a network immediately if your device prompts you with an insecure network notification.
- **Outdated operating systems (OSs):** If your device is running an outdated OS, it isn't receiving new security measures from the device manufacturer. Any mobile device that runs on an outdated OS will be exposed to more high-risk vulnerabilities as it becomes more outdated. Frequently check your device for updates, and install them as soon as possible.

**Hackers can use malicious apps, unsecured networks or a vulnerability in an outdated OS to access any of the information on a mobile device.**

BALDWIN KRYSTYN SHERMAN

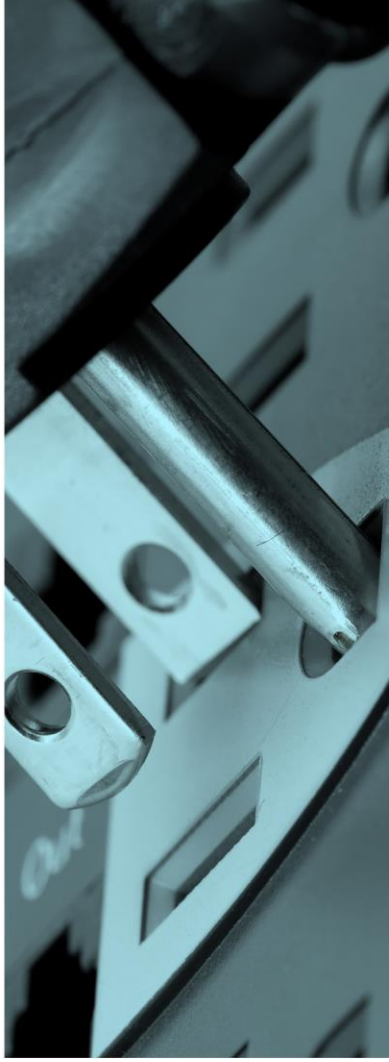
## Electrical Safety in the Workplace

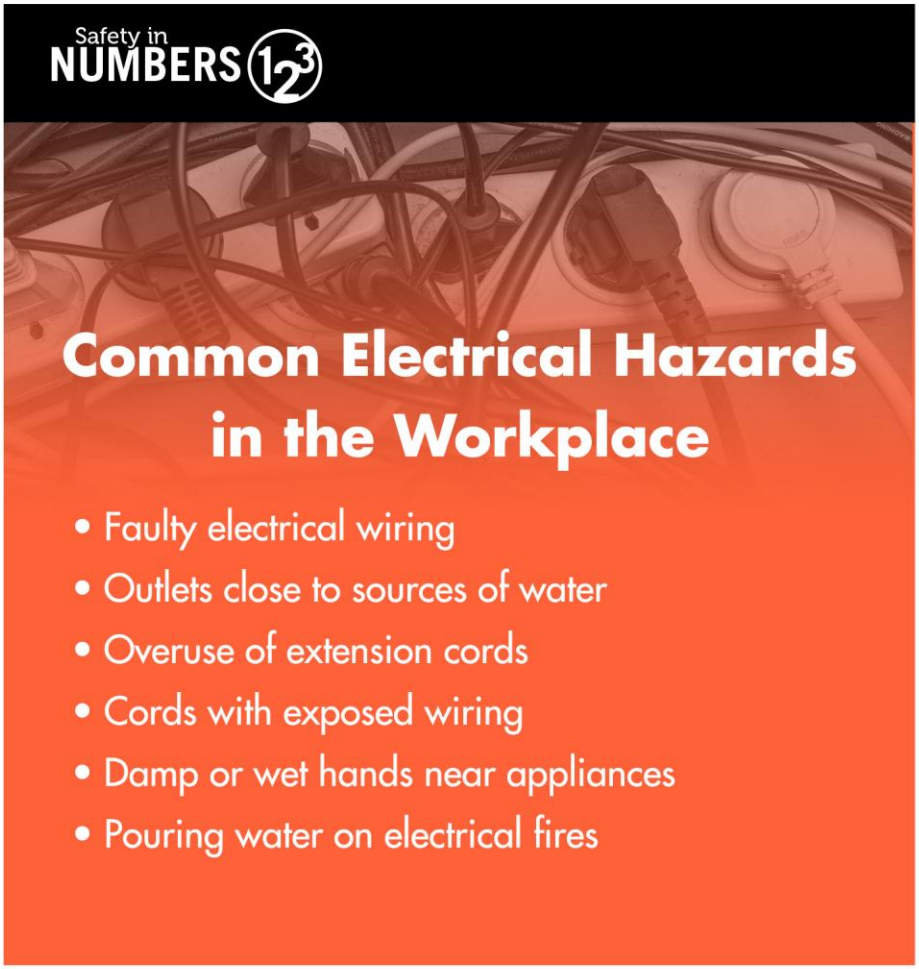
Although everyone uses electricity in the workplace, even a relatively small amount in an electrical outlet has enough power to lead to death by electrocution.

Any contact with exposed circuitry or energized appliances can interfere with the normal electrical signals in the body and lead to electric shock and burns. Additionally, if a shock occurs while an employee is on an elevated surface, muscle contractions or a startled reaction can lead to a dangerous fall.

Keep these simple tips in mind to stay safe around electricity in the workplace:

- Check electrical cords for damage before you plug them in. Cords that are even slightly damaged can lead to electrocutions and fires.
- Avoid overloading electrical outlets by only plugging in one high-wattage appliance at a time.
- Never plug in an appliance while it's "on" switch is engaged.
- Keep in mind that appliances that are turned off are still connected to electricity until they are unplugged.
- Unplug appliances from outlets by pulling on the plastic plug itself, not the cord.
- Take note if an outlet is unusually warm. This may be a sign that the outlet's wiring is unsafe, and it should not be used until it has been checked by a certified electrician.
- Never touch an appliance after an electrical accident. Instead, disconnect the power at the source first.
- Never use extension cords as permanent wiring. If your workplace doesn't have enough electrical outlets to reach all work areas, consider asking your manager to install more.
- Never use electrical appliances in wet or damp conditions.
- Place appliances that generate light or heat away from any flammable materials.






## Real-life Case Study

Jason, an outside sales representative, was traveling for business. During a layover at the airport, he decided to use his work phone to browse the internet. When Jason found that he couldn't access the airport's Wi-Fi for free, he found another open network that he could connect to.

While on the open network, Jason checked his work email and browsed some websites online, including his personal bank account. When Jason returned to his local office the next day, many of his co-workers told him that they had received suspicious emails that claimed to come from Jason himself. Additionally, Jason found that several strange charges had been made to his bank account since he had browsed on the open network at the airport.

Fearing that his work phone had been hacked, Jason decided to approach his manager. After an investigation, it was discovered that a hacker had used the open network at the airport to access Jason's work contacts and bank account. Since then, he has been careful to only use secure Wi-Fi networks and to keep his phone's OS updated.