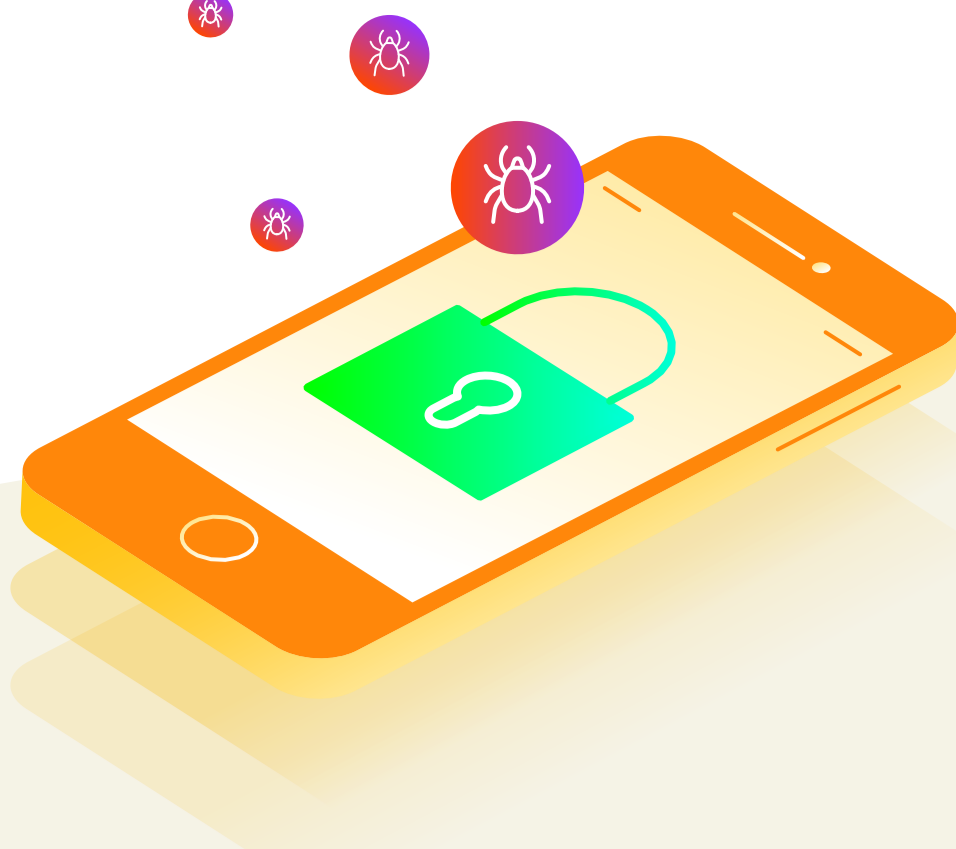


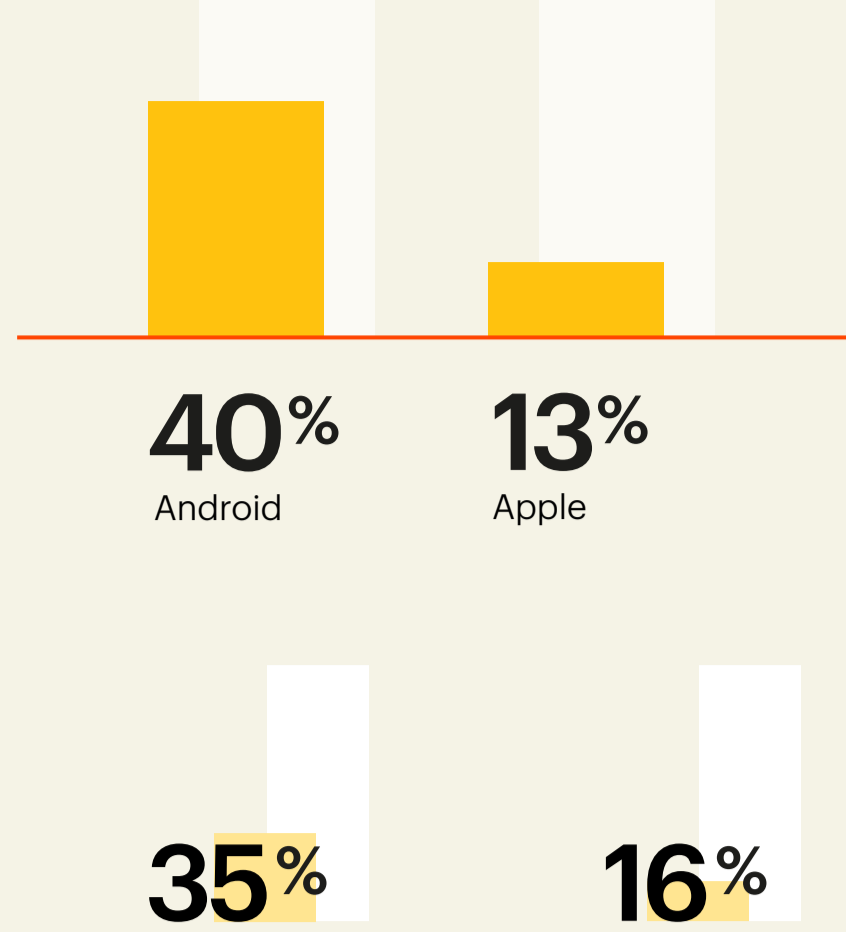
# Protect your mobile device

Our most vulnerable devices are in our pockets

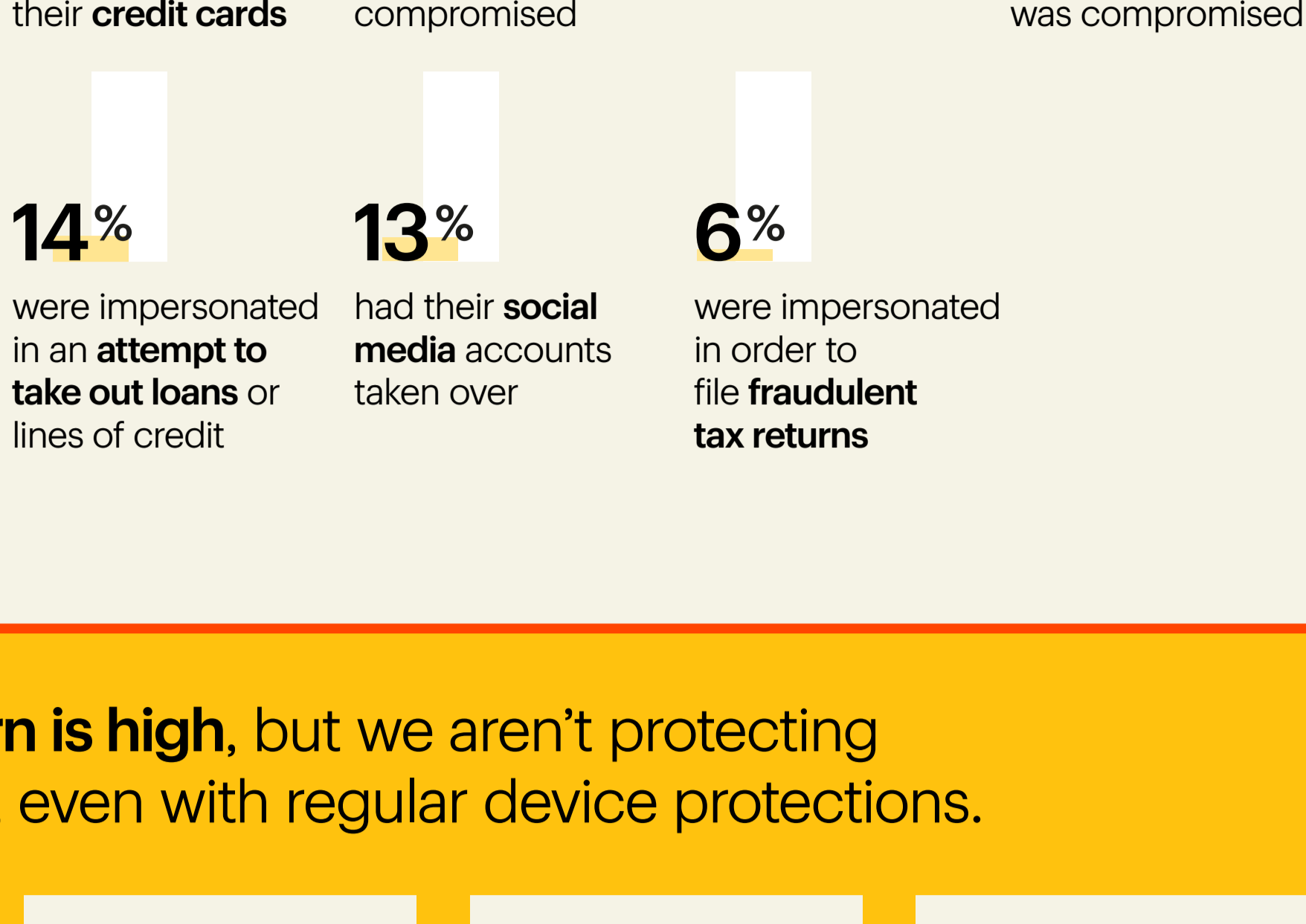


Mobile devices account for

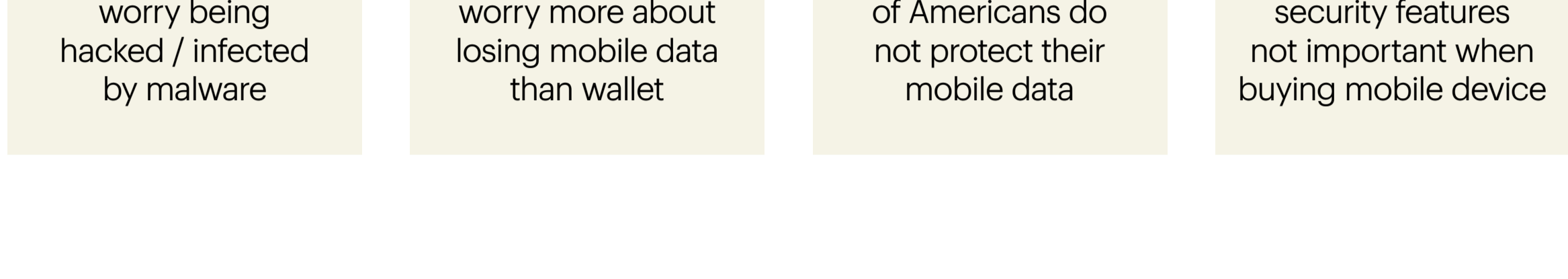
**53%** of internet usage



**64%** of Americans report being hacked

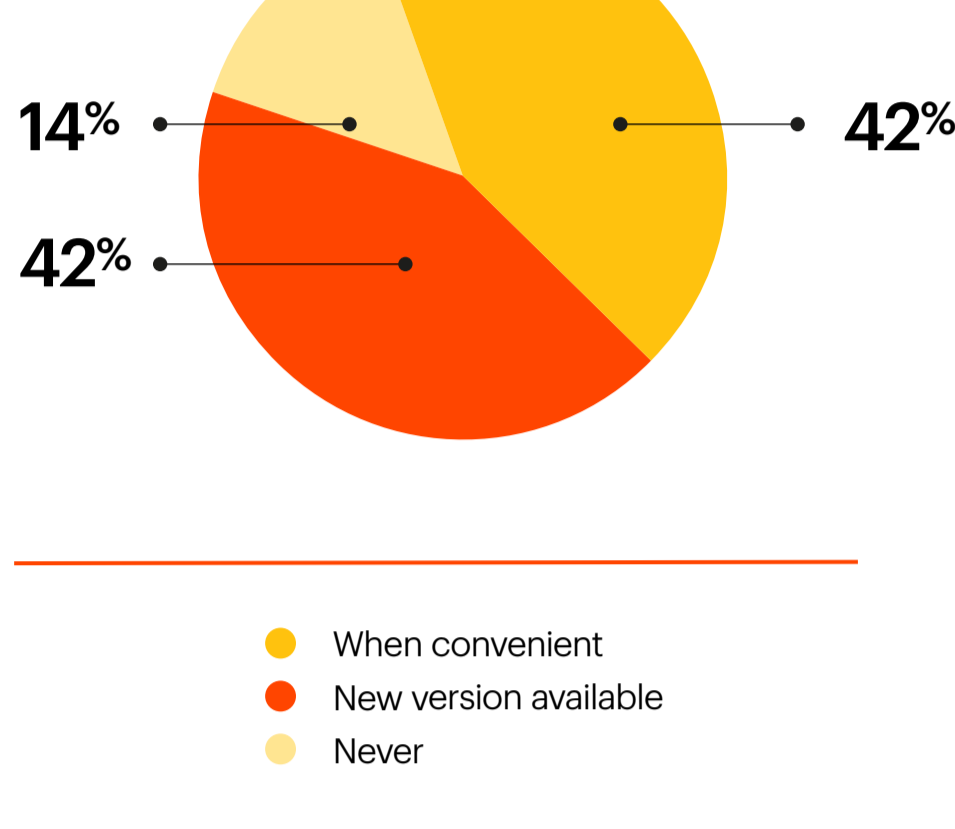


**Hacking concern is high, but we aren't protecting our mobile data, even with regular device protections.**

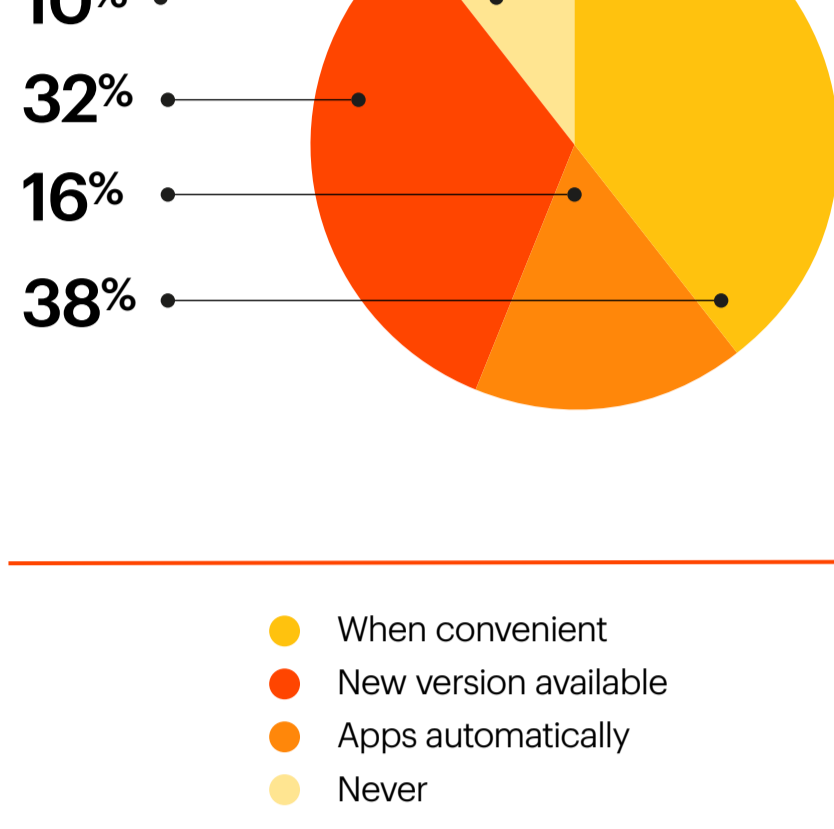


## Updating software

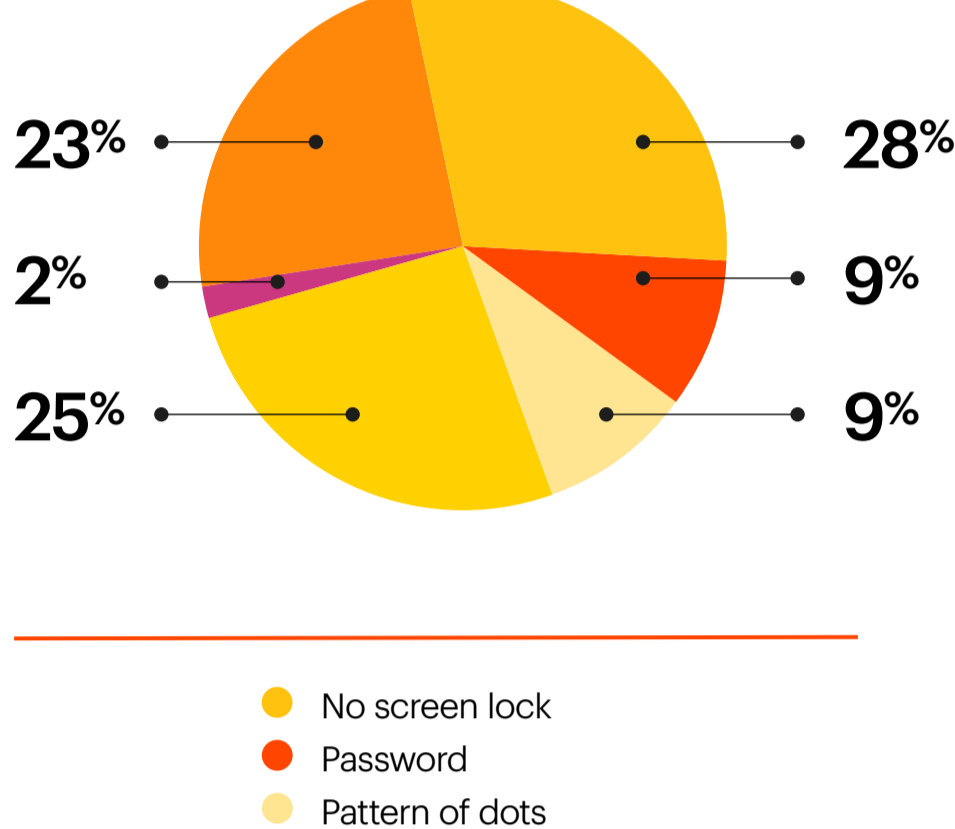
When do you update operating systems?



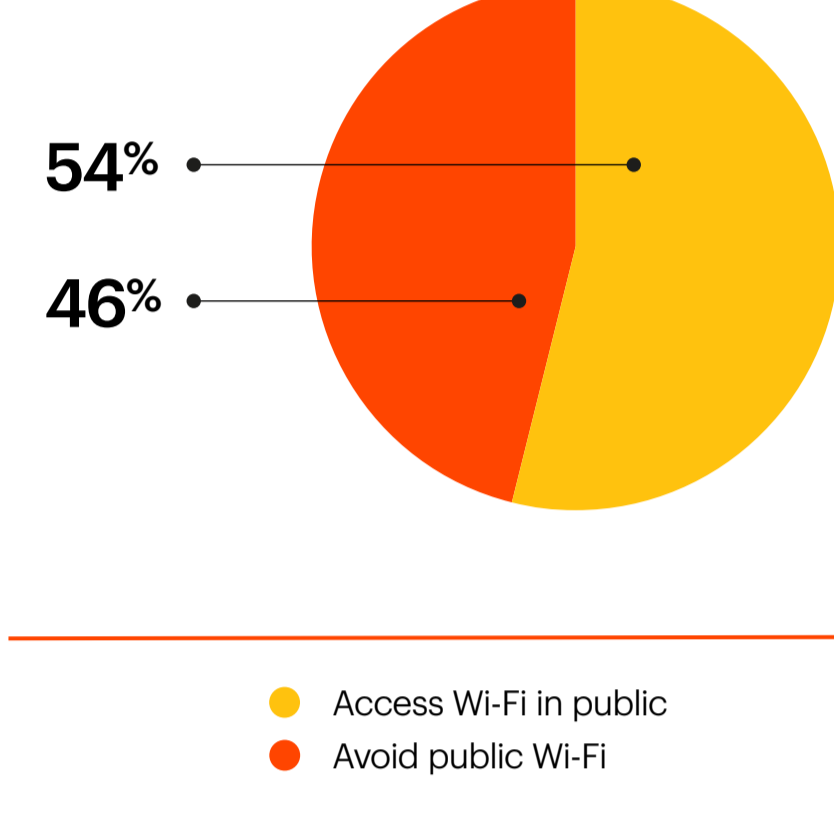
When do you update smartphone apps?



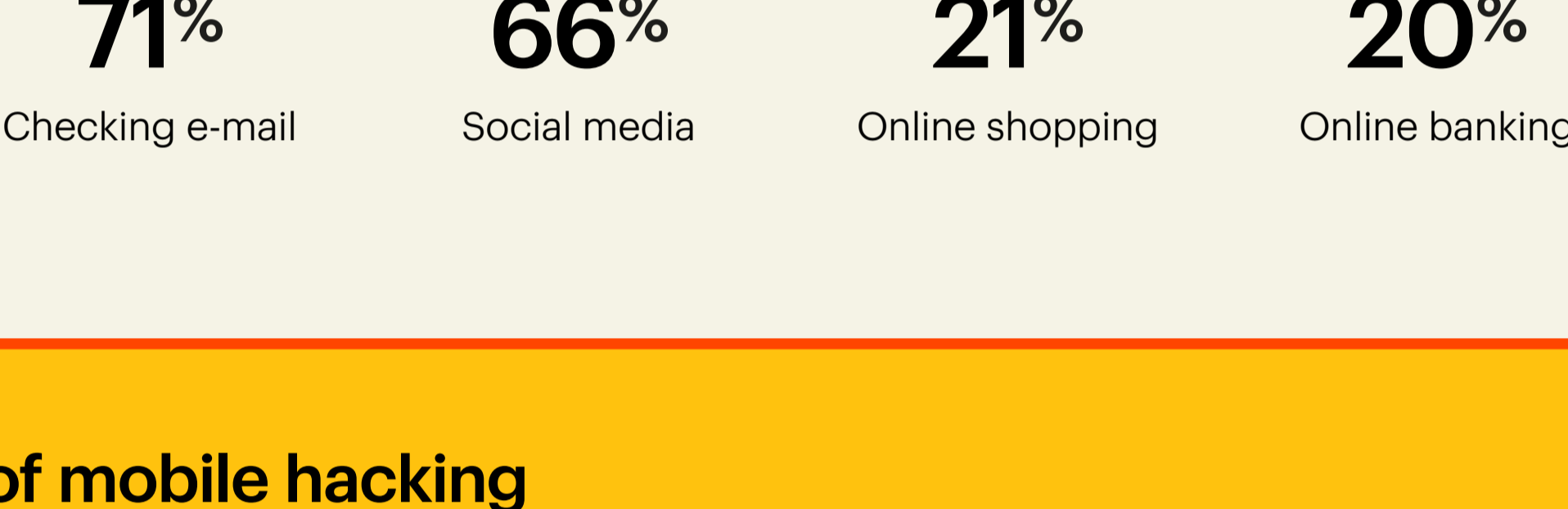
## Using screen locks



## Avoid public Wi-Fi



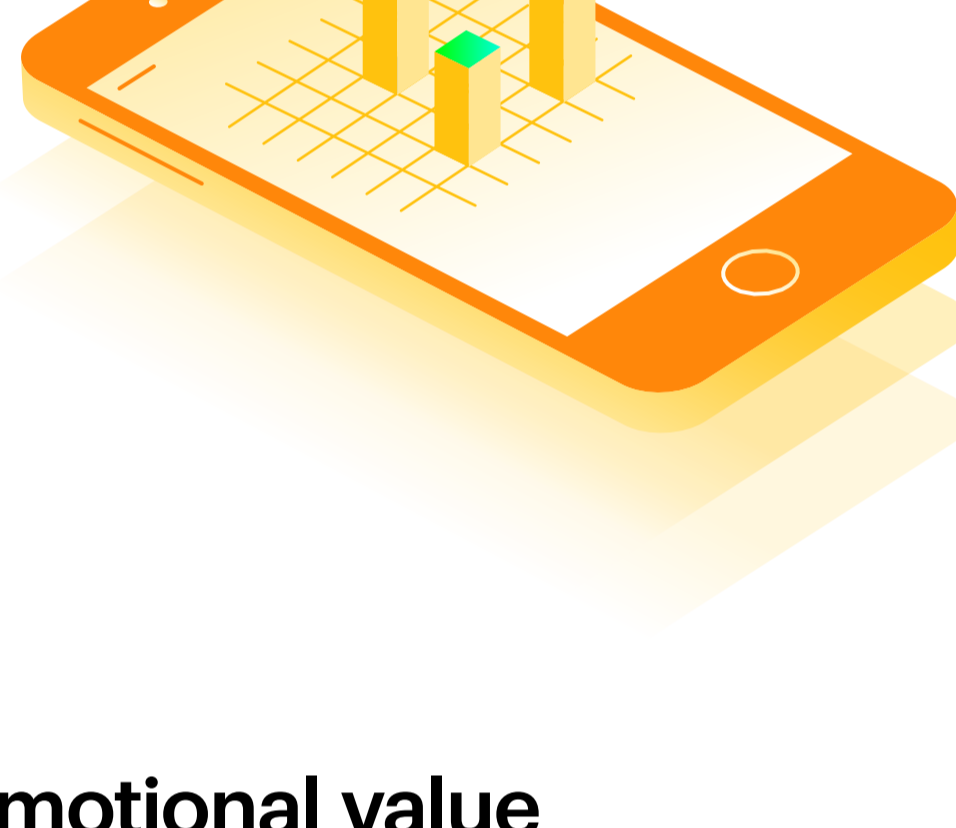
## How do you use public Wi-Fi



## Cost of mobile hacking

**\$14,000**

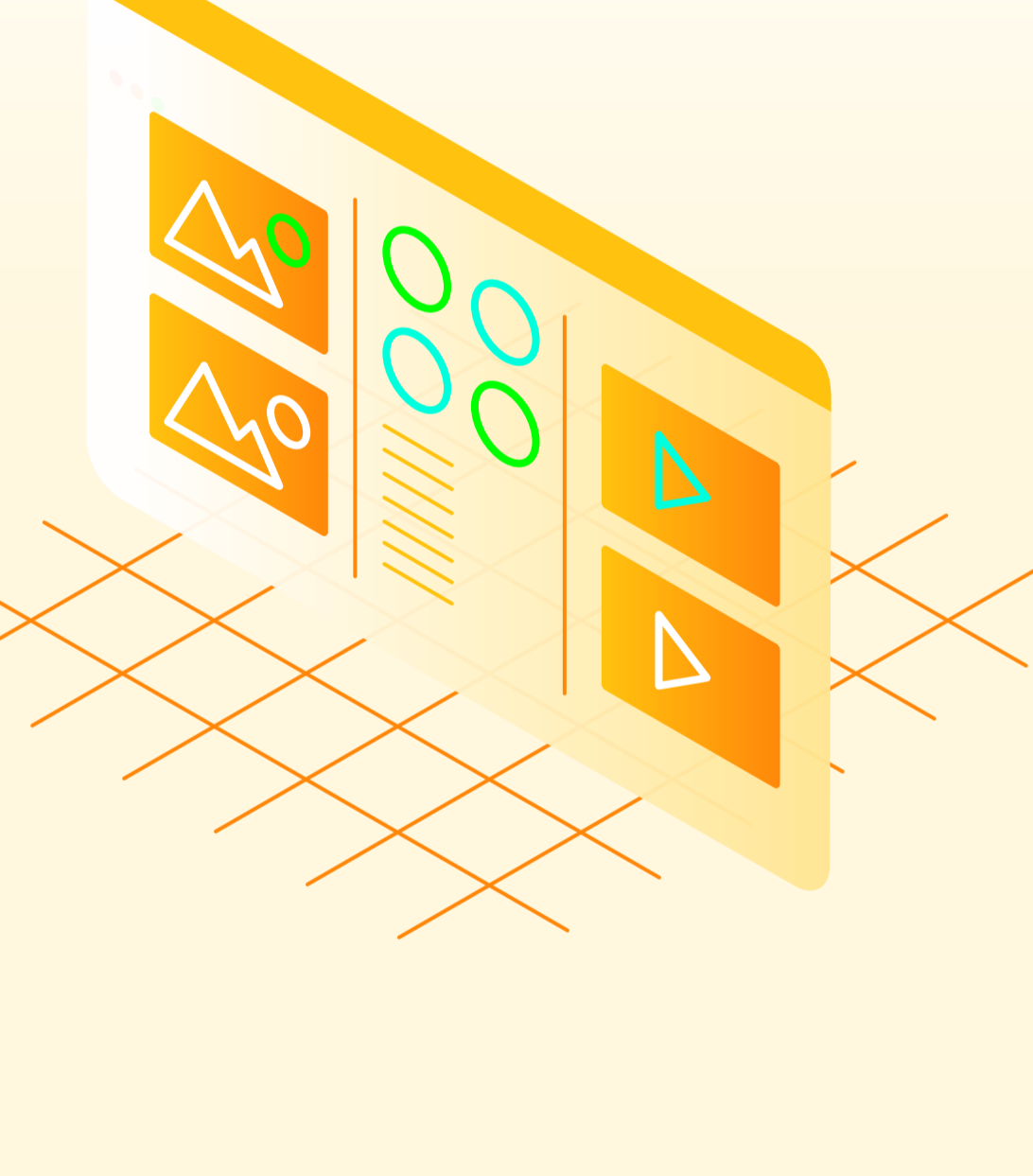
Average value of the data on a personal mobile device



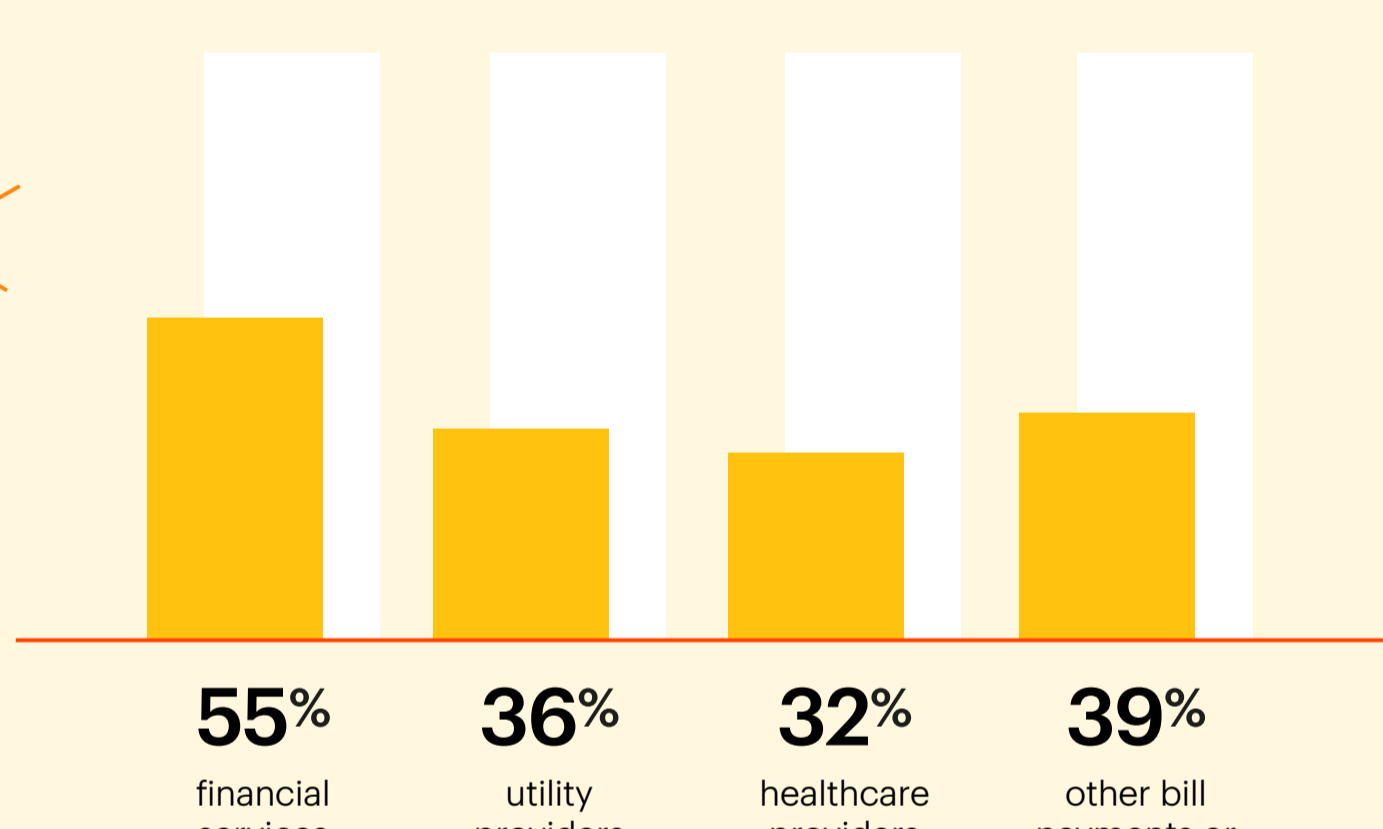
## Data of personal or emotional value

**47%** "The digital photos and video on my mobile device are priceless"

**50%** "I could never replace the content on my mobile device"

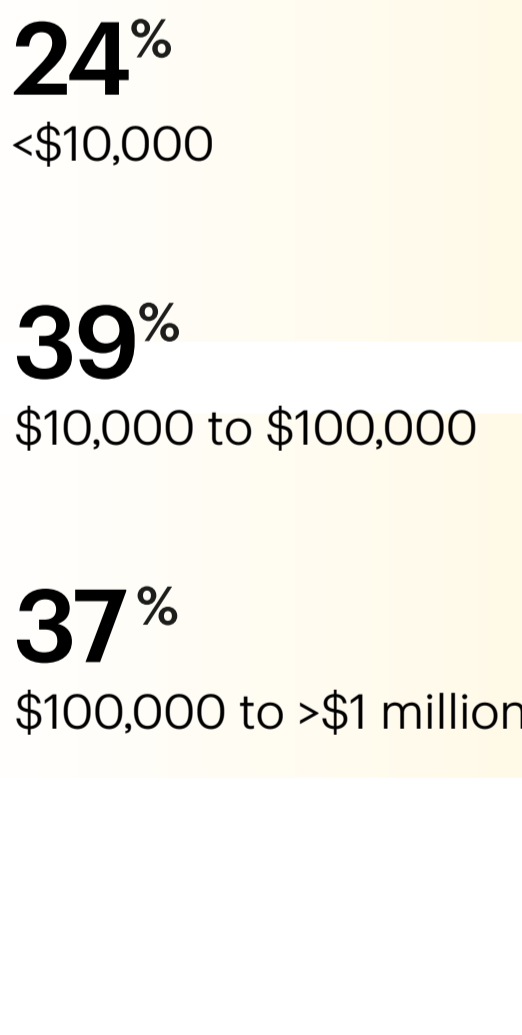


**2/3** of Americans have at least one online account with sensitive personal information



## Compromise employer data

### Cost of employee mobile device breach to a corporation



**64%** security professionals doubt their organizations can prevent a cyberattack from employees' mobile devices

**94%** of security professionals expect the frequency of mobile attacks to increase

## Types of mobile device hacks

**Spoofing**  
Misleading or unsecured Wi-Fi  
Hacker can create a similarly named Wi-Fi signal.  
Users connect to it thinking it is legitimate.

**Malicious apps**  
Free apps with hidden malware can compromise data.  
Download apps from the app store, not from messages or websites.

**Exploiting outdated operating system**  
Developers continually fix OS security flaws.  
When OS isn't updated frequently, phone is open to attacks.

**Man-in-the-Middle attacks**  
Interrupts communication between mobile device and internet.  
Could give a hacker access to your **data, messages and conversations.**

**Phishing**  
Friendly-looking emails or text messages with malicious links can gather sensitive information and install malware.

Only devices with mobile security apps **detect man-in-the-middle attacks and malware.**

## Install a mobile threat defense app

- Install software updates**
- Install apps from legitimate sources,** such as the App Store or Play
- Lock your device**
- Use different passwords** for accounts
- Don't perform sensitive tasks** on public or unsecured Wi-Fi

## How to know if you've been hacked?

- Works slowly** because of extra malware code
- Gets hot and battery drains quickly**
- Strange messages**
- Unfamiliar apps and popups**
- Consumes more data**

## Sources

gs.statcounter.com/os-market-share  
ibvresearch.com/global-mobile-security-market  
cbsnews.com/news/60-minutes-hacking-your-phone  
alliedmarketresearch.com/mobile-accessories-market  
pewinternet.org/2017/01/26/americans-and-cybersecurity  
gs.statcounter.com/press/android-over-takes-windows-for-first-time  
zenithmedia.com/26-of-media-consumption-will-be-mobile-in-2019  
inc.com/joseph-steinberg/14-signs-your-smartphone-or-tablet-has-been-hacked.html  
komando.com/tips/6339/5-ways-your-smartphone-can-be-hacked-without-you-knowing/all  
information-age.com/what-are-mobile-man-middle-attacks-and-how-dangerous-are-they-123461071  
theguardian.com/technology/2017/mar/26/12-ways-to-hack-proof-your-smartphone-privacy-data-thieves  
ponemon.org/local/upload/files/How%20much%20is%20the%20data%20on%20your%20mobile%20device%20worth%20Final%202010.pdf

Mobile security apps use artificial intelligence software to detect malicious behavior and malware on your smartphone. Once your device has been compromised, experts agree you should toss it!

**Is your smartphone or tablet secure?**

## Let's talk

Find out what Sprint Security Solutions can do for you. Contact your local Sprint representative today to learn more. Call 1-877-633-1102 or see more details on [sprint.com/business](http://sprint.com/business)