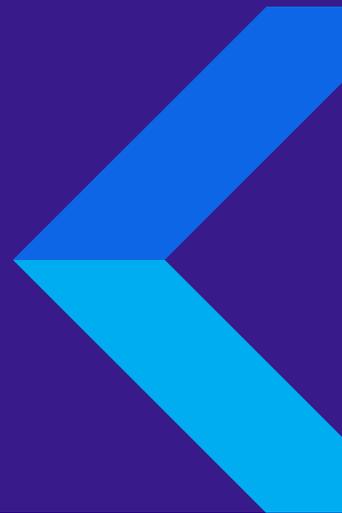




The Myth of Mobile Phone Privacy

Unlocking True Privacy for Sensitive Mobile Content



keepsafe

Don't Be Dumb About Mobile Content Privacy

Smartphones continue to become central to our lives — in the way we interact, conduct work, and access content. More importantly, smartphones have transformed the way we store content and information. But our reliance on our phones leaves a staggering amount of private information vulnerable.

What's stored on your phone?

- Photos? Videos? Texts? Work emails?
- App login credentials? Auto-fill information for your web browser?
- Mobile banking or personal apps with financial and account information?
- Emails to your accountant with personal tax information?
- Medical information you sent to your spouse or loved one?

Not surprisingly, many people use their mobile devices for at least one of these purposes every day. What is unexpected, however, is that most people aren't considering how to protect the private content that's at risk on their phones.

When it comes to personal photos, confidential work documents, ATM pins, and email passwords — people may be handing all of these over when they hand over their phones.

We Asked, You Told

To learn more about the sensitive content people keep on their mobile devices, we surveyed 1,000 U.S. consumers.

We wanted to know whether people are aware of how much private information is saved on their phone and what steps they're taking to safeguard it.

Alarming Lack of Phone Privacy

Not Private

70% think personal content and information on their mobile device is somewhat or not at all private

Sharing Passcodes

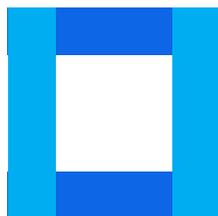
66% have given their phone passcode to someone else

For Anyone To See

50% don't believe they have content or information on their phone that they wouldn't want someone else to see (despite using phones for sending work emails and using mobile banking, payment and shopping apps)

Unlocked Phones

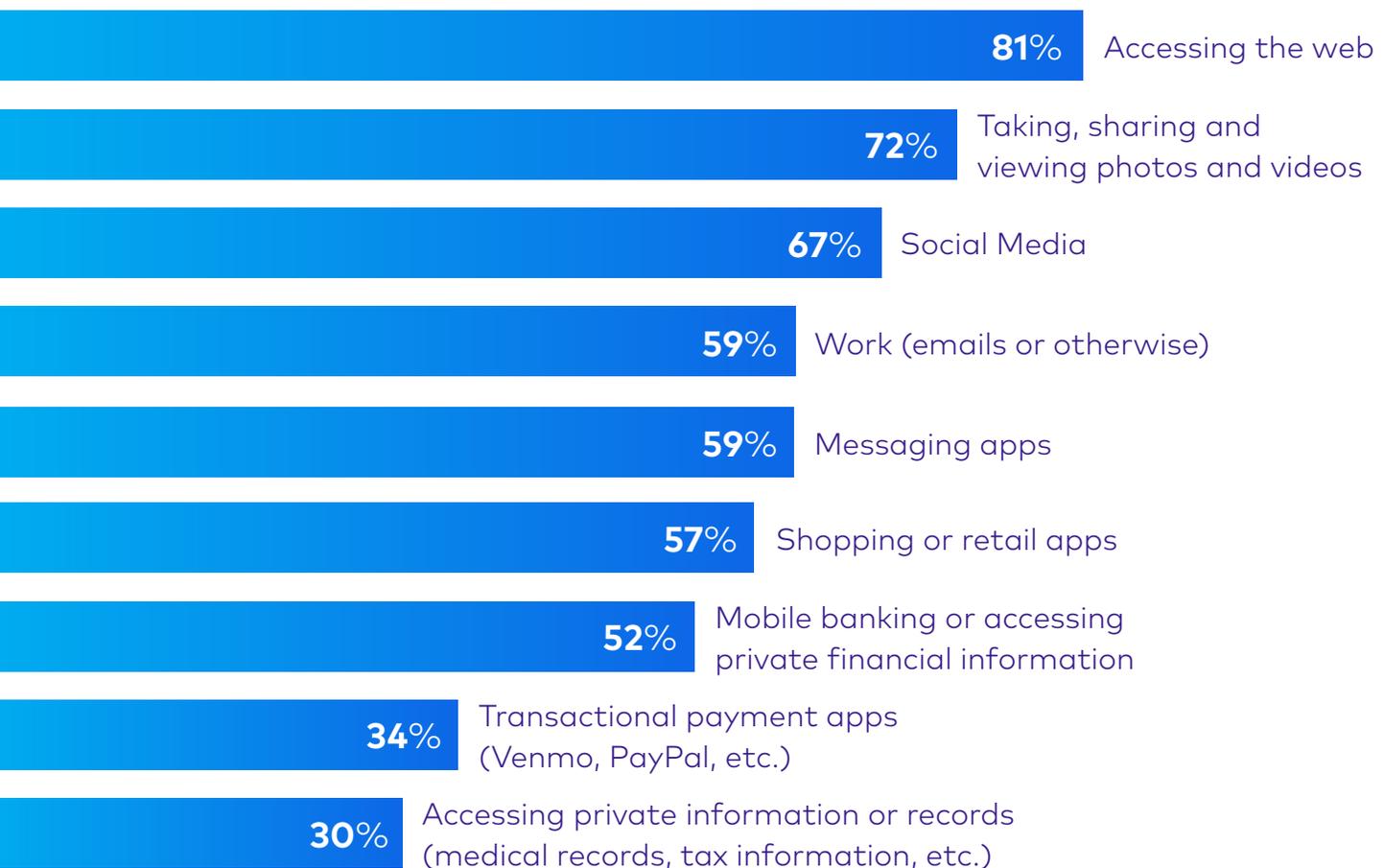
74% have handed their phone to someone unlocked, leaving themselves open to privacy breaches



People Can't Live Without Their Phones

As smartphones have become ubiquitous, our dependence on them has followed suit. In fact, 2015 research from Gallup found that 46% of people now say they can't live without their phones¹. In looking at how people use their phones, a clear picture emerges of just how much content and information resides on their devices.

People rely on their phones for everything:



¹<http://www.gallup.com/poll/184085/nearly-half-smartphone-users-imagine-life-without.aspx>

We're Concerned About Personal Privacy

Because people use their phones in a myriad of ways that require private content and sensitive information, surely they feel that content and information is safe, **right?**

Wrong.

Many consumers showed concern about the privacy of that information, acknowledging that they don't think their content is private. Others seemed unaware of sensitive content stored on their phones, and even expressed indifference to its privacy.

Confusion Over Phone Content Privacy



Not Private

70% believe personal content and information on their mobile device is only somewhat or not at all private



Don't Know, Don't Care

1 in 10 say they don't know or care if personal content and information on their phones is kept private



For Anyone To See

50% of people with work emails, mobile banking, payment and retail apps believe they don't have information on their phone that they wouldn't want someone else to see



Locked Up

Yet **71%** keep their mobile devices locked with a passcode



Few Safeguards

Whether or not consumers are aware that there's sensitive content on their phones, they still show a disregard for putting safeguards in place to protect themselves.

People Protect Their Sensitive Information:

- 87%** don't give out their **social security number**
- 86%** don't give out their **credit card number**
- 85%** don't give out their **ATM pin**
- 84%** don't give out their **email password**
- 73%** don't give out their personal **computer password**

Each of these credentials are kept more secret than mobile passcodes, but is it all for naught? **Isn't all this information at risk when mobile devices are left vulnerable?**

A minority of people still don't lock their mobile devices with a passcode, but alarmingly, the majority of those who do use passcodes make their mobile devices vulnerable by giving out their passcodes and handing over their phones unlocked.

People Still Share Passcodes and Unlocked Phones

				
Unlocked	Nothing To Hide	Sharing Access	Passing Around	Stranger Danger
1 in 3 do NOT keep their phones locked with a passcode	1 in 5 say there's nothing private on their phone	66% have given their phone's passcode to someone else	74% have handed their phone to someone unlocked	1 in 4 have handed their unlocked phone to a stranger

Millennials Value Passcodes, But Don't Protect Them

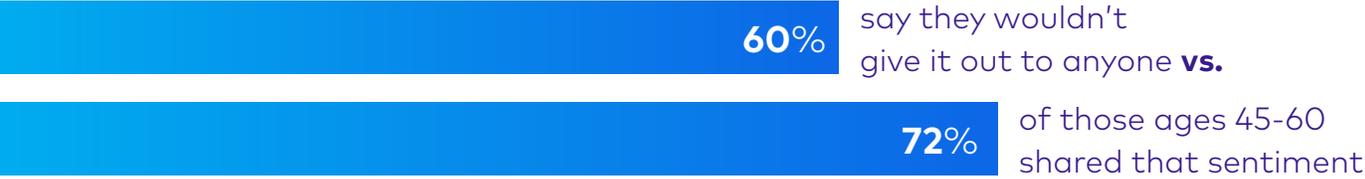
As digital natives, we assume millennials inherently understand their reliance on technology and its risks. But a closer examination of their mobile phone behavior reveals that this is not the case.

The younger generation uses mobile passcodes more than older consumers, but also share their passcodes more frequently. Millennials also often hand their phones to other people while they're still unlocked. The data shows that younger consumers aren't thinking about *how much* sensitive content they're putting at risk when they hand over their passcodes and unlocked devices.

Millennials Leave Phones Vulnerable



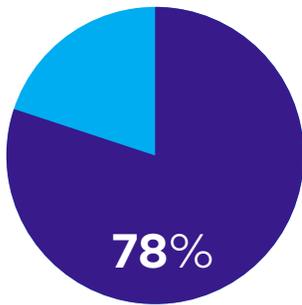
While millennials are more likely to lock their phone with a passcode (**84%** say they do); they are also more likely to share that passcode.



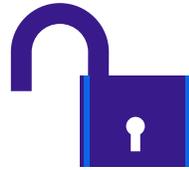
Despite **60%** of millennials saying they keep their mobile passcode private:



Though **48%** believe there *is* private content and information on their phones



have handed their phone to a friend while it was unlocked



At The Office

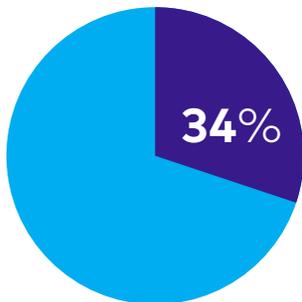
1 in 3 have handed their phone to a coworker unlocked



Stranger Danger

1 in 3 have handed their phone to a stranger while it was unlocked

Although the majority of millennials say they use their phone for texting, taking and sharing photos and videos, using social media, working, mobile banking, accessing the web, and shopping:



of millennials don't believe they have any private content, data or information on their phone that they wouldn't want someone else to see



They Don't Know

1 in 5 don't know or have never thought about whether they do

Leaving Content and Information Vulnerable

It's worth taking a closer look at just how vulnerable the content on mobile devices really is. Few people would be comfortable leaving their wallet open or having sensitive work documents out in the open for anyone to see. So consider the potential ramifications if login credentials or credit card information are saved on phones. Think about the increased vulnerability if sensitive company information is readily accessible on phones.

Mobile Bankers are Putting Their Information At Risk

\$\$\$
Of those who use their phone for mobile banking:

- 64%** have shared their passcode with someone else
- 1 in 4** think the information and content on their phone is not private
- 41%** believe they don't have any personal or private information or content on their phones that they wouldn't want someone seeing

Sensitive Company Information Potentially Exposed



Of those who use their phone for work:

- 1 in 5** do not keep their phones locked with a passcode
- 63%** have shared their passcode with someone else
- 49%** say they only somewhat think the data, content and information on their phones is private
- 44%** say they don't have any personal or private information or content on their phones that they wouldn't want someone seeing, and another 8% say they don't know if they do

People Aren't Protecting Financial Information



Of those who use their phone for payment apps (Venmo, PayPal, etc.):

- 1 in 5** do not keep their phones locked with a passcode
- 62%** have shared their passcode with someone else
- 1 in 4** admit the content and information on their phones is not private

Pay Better Attention to Content Privacy

Given the multitude of ways that people use mobile devices, and the private content that lives on their phones as a result, consumers demonstrated a lack of concern for their privacy. Sensitive content is left vulnerable when people don't use passcodes, share their passcodes, and hand over their phones unlocked.

The implications are staggering, as inadequate safeguards leave personal photos, messages, work emails and documents, financial information, and other personal information susceptible if a mobile device lands in the wrong hands.

Consumers who say that they're protective of their social security numbers, ATM pins, and email passwords must also think about the information that those codes protect, and where else that information is readily available — because chief among them is their mobile device.

Methodology:

Keepsafe surveyed 1,000 U.S. consumers in November 2016 through an online survey. Responses were random, voluntary and anonymous.

About Keepsafe

Keepsafe makes privacy in the digital world simple. 50 million people use Keepsafe's secure vault to protect their private photos, videos, and documents. For consumers who want more control over their privacy, the freedom to be themselves, and peace of mind, Keepsafe locks down personal items so they stay private.