

CPIQ

Consumer Privacy & Identity Quarterly

The Tech Between Us
New Digital Communication
Tools Connect Friends, Families

Changing Tech, Changing Habits
Curating Safe Communication Habits
Amid Constant Technological Change

Bugs and Breaches
Privacy Risks in Staying Connected

The Great Juggling Act

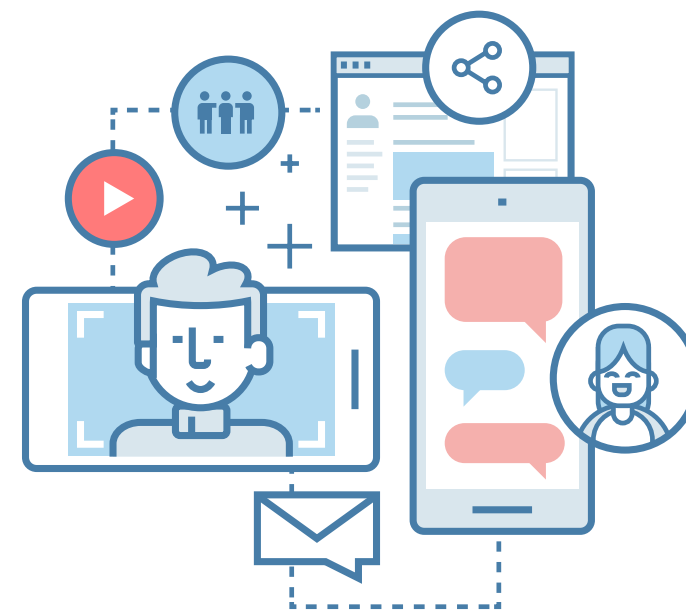
Staying In Touch in the Digital Age



VOLUME 4 ISSUE 2



In this Issue



- ## 2 CONSUMER PRIVACY & IDENTITY QUARTERLY

The Tech Between Us:

New Digital Communication Tools Connect Friends, Families



Are you curious about the state of digital communication today? Run a quick search of the most popular apps of 2018. On every platform, digital communication apps such as Whatsapp and Skype are among the most popular, garnering millions of downloads. Digital communication tools and companion services that enhance our modes of expression (Bitmoji anyone?) tend to make up 50% or more of the rankings, and almost always appear in the top five. Alongside entertainment services like video games and TV streaming, digital communication tools are the most likely items to be taking up the average person's time online.

This popularity is driven by necessity and irresistible convenience. Our day-to-day social interactions, once limited by geography, now span the globe. Travel, work, and relocation increasingly take people farther from family and friends. Odds are, many of your important contacts are a plane ride away, but keeping up with them is no problem. The previously costly and limited long-distance communication methods we once relied on have been replaced with a multitude of free ones.

Digital communication technologies make separation more tolerable. The field is bursting with innovative solutions for keeping up with far-flung family and friends, and people have rushed to adopt them. In previous decades, deployed military personnel resorted to letters and perhaps an occasional, poor-quality long-distance phone call to reach relatives. In 2018, the 165,000 active-duty military personnel stationed abroad had access to dozens of high-performing technologies to keep in touch: voice calling, video calling, messaging, and photo sharing

services, just to name a few. Rather than sending postcards with a few short sentences, traveling parents can now send daily voice messages to kids using a stuffed animal with a built-in sound chip that links to an app. Basic phone calls—even ones with crystal clear reception—seem underwhelming in comparison.

With so many digital communication options, users should consider their personal interests, preferences, devices, and data plans, along with those of their contacts, in order to determine which tools suit them best. But at the end of the day, it's difficult to balance all these complex decision points and still find the motivation to think critically about the safety, security, and privacy of each communication channel at your disposal.

This CPIQ issue aims to help readers successfully navigate today's state-of-the-art digital communications market, while preserving a healthy degree of user privacy. The feature presents a landscape overview of messaging apps, which anchor the global digital communication market at a time when many people prefer texting to talking. Subsequent articles present strategies for optimizing your digital communication toolbox for both utility and privacy, ensuring safe correspondence for both you and your loved ones. You will learn how to protect yourself while traveling, what communication apps are ideal for kids, and how encryption actually works. We close by considering how the debut of radical new technologies—burgeoning developments in augmented and virtual reality domains, underpinned by the rollout of advanced 5G networks—will shape our interactions in the near-future.

Bugs and Breaches: Privacy Risks in Staying Connected

Despite concerns that people are “talking” less face-to-face, we are communicating with each other more than ever. According to the 2019 Cisco Visual Networking Index report, the average mobile data traffic generated globally in 2018 was 19 billion gigabytes per month; this figure is expected to reach 77.5 billion in 2020. Digital communications account for a significant portion of this traffic, and the resulting data trails—including contact lists, chat histories, and SNS archives—provide valuable entry points for theft and exploitation of identity and privacy.

Let's review common communication risk scenarios and ways to prevent your identity from being compromised.



Scenario #1: “I Was Part of a Data Breach”

Telecommunication service provider breaches reveal personally identifying data that can construct a person's robust social universe. In a recent breach, Voipo, a VOIP provider, exposed millions of customer call logs, SMS messages, contacts, and credentials. If you become aware of a data breach, immediately notify your contacts, delete the account, and update your access credentials on other apps.

Scenario #2: “My Messaging App Contains a Security Bug”

Apps are all prone to bugs, even apps that are deployed across 1.4 billion active devices. Apple came under fire in early 2019 when a FaceTime bug allowed callers to listen in to other people's conversations and even see video without their knowledge. Run software updates for your apps and phone OS frequently to ensure you are protected against recent security vulnerabilities.



Scenario #3: “My Communication Device is Malfunctioning”

It's not just your app that's vulnerable to hacking. Internet of Things (IoT) devices ranging from the 2017 Amazon Echo to CloudPets' fluffy baby-monitoring teddy bears contained vulnerabilities that could allow outsiders to remotely listen in on any conversations happening within hearing range. If a device security malfunction is exposed, stop using the device immediately and update to a newer, more secure model.



Changing Tech, Changing Habits

Curating Safe Communication Habits Amid Constant Technological Change



The variety in today's market makes it challenging to pick one main digital communication tool, or even a handful. Important factors change as your lifestyle evolves—you upgrade your phone, and download trending apps to see if you like using new communication formats. The mental burden increases when apps change Terms of Service, when service providers acknowledge a data breach, and when different services merge, such as WhatsApp, Instagram, and Facebook Messenger.

As soon as you launch a new app, you're busy corresponding. Odds are you're receiving notifications while reading this article; no wonder it's hard to find time or energy to consider safety and privacy implications.

Tedious though it is, taking the time to carefully think through your digital communication habits offers major payoffs—helping to protect your privacy and sensitive identity data. Here are some main points to consider:

What are you communicating? Whether you're sending text, photo, or video calling...

- Be sensible! The convenience is tempting, but it's inherently risky to send sensitive info via apps on unsecured Wi-Fi or mobile networks—especially when you're communicating with someone abroad. Remember that most of your digital transmissions can be recorded, hacked, or shared. Furthermore, many services store your communication data in the cloud, and can access and review your logs. So think hard before you do something like exchange PII with a deployed spouse over your favorite messaging app.
- Don't needlessly overshare. Many messaging apps incorporate additional features that can reveal a lot about your life. Turn off location-tracking features (unless specifically needed for safety purposes). Avoid linking your mobile number when not required, and skip filling in optional profile information.

- Delete conversation histories when you conclude a correspondence, or at regular intervals (e.g., every three months).

How are you communicating? Have you fully secured your digital communication channels?

- Run routine updates for your apps, router firmware, and device operating systems.
- Install and run antivirus software, even on your smartphones and tablets.
- Use apps that offer end-to-end encryption, and VPNs when you're online on-the-go.
- Conduct routine maintenance. Your app preferences and needs change naturally over time, so deactivate unused accounts and remove old apps from your devices.

With whom are you communicating? i.e., KonMari your contacts...

- Curate your contact list. Connect only with people you know and plan to engage with routinely; remove inactive connections when you fall out of touch.
- Scale your sharing by platform. For example: instead of sharing pictures of your recent family reunion with all your Facebook friends, use a more specialized app that supports family-only sharing (e.g., TinyBeans).

When and Where are you communicating? Now that it's almost too easy to engage anywhere, anytime...

- Consider your environment and ensure you're not disclosing sensitive information at home, work, or in other private settings. For example, FaceTiming a friend from your office may lead to inadvertent disclosure of proprietary corporate information.
- Disconnect occasionally: continuous communication is great, but remember to spend unplugged quality time keeping up with loved ones IRL (in real life).



TOP FIVE Communication Apps for Kids and Parents

Kid-focused communication apps have become increasingly common as more elementary school-aged children use smartphones and tablets. Here are five parent-approved apps that help kids foster healthy online communication habits.

1

Mazu

Mazu is a family-oriented social media and messaging app in which parents monitor and approve all activity. Mazu adopts a "digital village approach" designed to teach children safe communication and social media etiquette in a controlled environment. This feature can be a valuable stepping stone in preparing children to navigate risky content and behaviors commonly encountered in larger, adult-oriented online platforms.

2

JusTalk Kids

JusTalk Kids, a simplified version of JusTalk, is a free encrypted text and video messenger app intended for children ages 3 and up. End-to-end encryption protects the content of calls and messages, and personal data is not shared with third-parties. Kids cannot see or accept friend requests without parental approval. No mobile number is required for app registration.

3

Messenger Kids

Messenger Kids is a free video calling and messaging app designed by Facebook. A child's Messenger account is created through a parent's Facebook account, enabling the parent to exercise full visibility and control over the child's shared content, friends, and message history.

4

GeckoLife

GeckoLife is a collaborative platform geared toward small groups—including families. All shared messages, images, and documents are private by default. Parental controls ensure that accounts can only be created by parents, and that parents receive notifications about kids' activity, posts, and connections. Using GeckoLife helps parents model and teach safe social media habits.

5

VTech KidiConnect

KidiConnect is a text and voice messaging companion service for the VTech KidiBuzz communication device. It allows parents to exercise full control over content and connections. Parents can also remotely remove apps and games from the KidiBuzz, control website access, and set screen-time restrictions.



The Great Juggling Act

Staying In Touch
in the Digital Age

The evolution of technology has always fostered humans' ability to communicate. Consider pre-industrial people, who used smoke signals, drums, horns, trail runners, and pictographs to communicate across moderate distances. The influential invention of paper in 100 A.D. allowed humans to communicate through written correspondence. The introduction of the postal service later enabled individuals to have private conversations without being in the same vicinity.

Fast-forward to 2019—past the invention of the telephone, personal computer, and dial-up Internet. Today, we can communicate instantaneously with anyone across the globe, using new communication technologies being introduced at a rapid rate. Advancements in cellular networks and smart devices have afforded us a level of connectivity we have never experienced before, but they have also afflicted us. We now face an overwhelming number of options for completing the formerly simple and joyous task of staying in touch with family and friends.

A typical user today juggles different modes of hardware and software to communicate. On top of using basic smartphone text and call features domestically, a well-connected user may speak to in-laws in Europe on WhatsApp, use Signal to touch base with privacy-conscious friends, chat on Facebook Messenger with acquaintances living in Berlin, and use KakaoTalk to check in with extended family in South Korea. Each time you send a message, you must solve a quick riddle: figuring out what platform (Which app or service should I use?) and what media you should include (Should I text, call, video call, or send a GIF?), based on the recipient's communication preferences. At times, something as rudimentary as reaching out to a good friend can feel exhausting.

Rise of Data-Based Messaging Systems

How did we end up in a fiercely saturated market for personal communication? After all, text messaging, once known as short message service (SMS), used to be the only way to send messages via phone. The options were fairly simple for keeping in touch: you could either call or text.


The arrival of smartphones marked the beginning of data-based messaging systems reliant on 3G, 4G, and Wi-Fi, rather than the universal 2G cellular network which SMS messaging uses. SMS can be sent and received on any phone, smart or not, but for a fee (and even more when you're sending messages internationally). In contrast, data-based messaging systems made sending messages completely free and rapidly grew in popularity.

Modern Messaging Apps

Globally popular services like WhatsApp, Telegram, Viber, Line, Snapchat, and China's WeChat are all examples of data-based messaging platforms. They are either stand-alone platforms that enable messaging using network data, or spin-offs from existing social networking platforms such as Facebook Messenger. They are the most widely used smartphone apps today, with over 1.3 billion monthly users on WhatsApp and Messenger combined.

Many of the messaging apps evolved into broad platforms that enable social network service (SNS) features such as status updates, chatbots, payments, and e-commerce via chat. WeChat's conversational commerce—e-commerce through the use of messaging—has grown so much that users can buy everything from music to a brand-new car. Messaging apps incorporate some of the following versatile features:

- Chats
 - > One-on-one (1:1) chat
 - > Group chat
 - > Broadcast lists
 - > Chatbots (including "bot in group chats")
 - > "Smart replies" (suggested replies to incoming messages provided by Google's Reply platform)
- Calls
 - > Voice calls
 - > Video calls (1:1 or group)
- File sharing, e.g., Slack
- Games
- Payments or mobile wallets
- Personal Cloud Storage
- Status updates



Additionally, diversifying your contacts and conversations across different apps is a good privacy practice as it prevents all your information from being exposed when an app inevitably suffers from a major privacy leak.

Never heard of it? Wildly Popular Country-specific Messaging Apps

Though popular in the United States and Europe, WhatsApp and Facebook Messenger haven't quite taken over the whole world yet as they like to claim. The three biggest economic powers in East Asia have their own country-specific messaging apps that dominate market penetration and usage in their respective countries and elsewhere in Asia.

WeChat is China's most popular messaging app, and one of the world's biggest with 938 million active users. It functions as a multi-purpose platform with SNS features and a robust mobile commerce marketplace. WeChat is subsidized in part by the Chinese government and has been accused of censoring and monitoring politically-sensitive communications; approach with caution when trying this app.

South Korea's favorite messaging app is **KakaoTalk**, used by 95% of the country's smartphone owners. It has 220 million registered users and is available in 15 languages, including English. It contains SNS and commerce features, including a ride-sharing service called KaKao T.

In Japan, **LINE** was rolled out as a disaster response app after the 2011 earthquake and tsunami and has since grown into a multi-purpose messaging app. Today it has 500 million users across Japan, Thailand, Indonesia, and Taiwan. In Japan, it's used by 92.8% of the country's mobile messaging app users.

- Live-streaming, e.g., Line, Instagram
- Stickers, e.g., Emoji, Bitmoji
- Virtual assistant, e.g., Google Assistant in Google Allo
- Encryption, e.g., Signal, WhatsApp, and Telegram

These rich features have expanded what it means to communicate. On a daily basis, people interact using multiple media types beyond simple calls and texts; friends send photos, videos, URL links, personalized avatars, and gifs to express their moods or check in with each other. Inviting acquaintances to play a game or sending someone a gift via chat are all considered legitimate ways of staying in touch. Also, people are accustomed to many modes of correspondence, from engaging in 1:1 chats or group conversations to sharing status updates, to creating livestreams with large or public audiences.

Messaging Remains a Competitive Sector

Unlike the majority of the technology sector where near-monopolies control specific domains—such as Google in search, and Facebook in social networking—messaging remains a fragmented market where each major player uses proprietary technology without offering options to communicate across platforms. People mainly use messaging platforms to maintain and strengthen existing social connections, as opposed to creating new ones, so there is less pressure to be "seen" or "discovered" by others. Users simply select and download messaging services that friends and family use. The pain of switching is particularly high as it requires convincing all your contacts to switch for the change to be worthwhile.

Diversity of Messaging Apps & Privacy

While there is reasonable nostalgia for the simple days of the universal SMS messaging system, the market competition created by modern apps has been generally positive from a privacy standpoint. SMS messages are never encrypted, which means they are viewable to mobile carriers and even semi-skilled hackers when intercepted.

In contrast, messaging app providers like Signal, WhatsApp, and Wire provide end-to-end encryption on all messages and calls, which means sent messages are scrambled on one end of the conversation—the device—and unscrambled at the other end, on the recipient's device. This makes it nearly impossible for anyone else to see what is being said. Additionally, diversifying your contacts and conversations across different apps is a good privacy practice as it prevents all your information from being exposed when an app inevitably suffers from a major privacy leak. The breach will only impact a portion of your personal contacts and correspondences as opposed to all.

The excess of modern communication tools can be annoying to sort through, but this pool of services has greatly improved accessibility, convenience, and privacy for most users. As with your financial investments, keep your digital communications diversified across a variety of platforms to protect yourself, your contacts, and most of all, your data.

FROM LETTERS TO LIVE-STREAMING: Tracing the Evolution of Digital Communication

THE TIME BEFORE

- Handwritten letters by post
- Landline telephones and phone cards for long distance calling
- Cell phones operated on 1G (analog)
- Fax machines led vanguard of digital technologies in the 1980s



1990s

- Dial-up Internet and PCs become popular, enabling common use of:
 - Email
 - Instant messaging (ICQ, 1996)
 - Peer-to-peer (P2P) sharing (Napster, 1999)
- The introduction of 2G digital telecommunications networks in 1991 and 3G in 1998 help foster the slowly growing cell phone market



Early 2000s

- 3G mobile networks enable rise of widespread cell phone ownership & usage:
 - SMS texting
 - Voice calling
- Improvement of web development tools along with Internet availability and performance enable:
 - Development of tablets
 - Launch of Skype, 2003
- New approaches to communication develop. The Internet becomes interactive and social. Communicating digitally can be as equally gratifying as in-person interactions
 - MySpace, 2003
 - Facebook, 2004
 - YouTube, 2005
 - Reddit, 2005



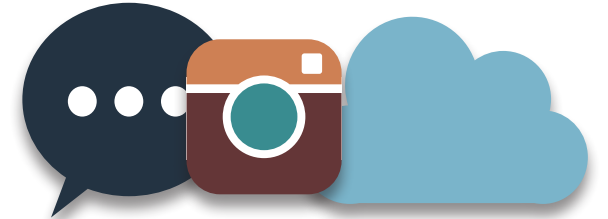
Late 2000s

- Internet accessibility and performance improves, particularly as Wi-Fi becomes commonplace. Smartphones become commonplace, allowing for constant connectivity. Mobile network capabilities give rise to:
 - Twitter, 2006
 - iPhone, 2007
 - Whatsapp, 2009



Early 2010s

- Internet and mobile network infrastructures continue to improve, as 4G/LTE rolls out in 2010, Wi-Fi hotspots continue to grow, and cloud computing increasingly enables remote storage of message histories. These developments facilitate new apps:
 - Instagram, 2010
 - Snapchat, iMessage, Facebook Messenger, 2011
 - Slack, Telegram, 2013
 - Signal, 2014



Late 2010s

- By 2016, half the world's population is digitally connected. Live-streaming becomes popular.
 - Periscope, FaceTime, Discord (voice and text for gamers), 2015
 - Facebook Messenger Kids, 2017
 - Facebook Portal, 2018



2020 & beyond

- 5G's increased bandwidth and low latency will enable:
 - Augmented and Virtual Reality
 - Facebook Reality Labs AR Glasses, Codec Avatars
 - Google Lens AR camera
- Major service providers seek to consolidate popular communication channels
 - Proposed integration of Whatsapp, FB Messenger, Instagram





A New Generation of Privacy Risks: The Future of 5G Internet

Picture this: it's 2022 and the new Game of Thrones prequel series is premiering. You and a friend want to watch together, but you are in New York and she is in Los Angeles. No problem. You call her, put on your augmented reality (AR) smart-glasses, and a computer-generated, real-time projection of her appears next to you on the couch—just in time to learn the true origin of the White Walkers.

The future, brought to you by 5G.

Rolling out this year, 5G—the wireless protocol that transmits data up to 100 times faster than 4G networks—will transform how we keep in touch with family and friends.

Augmented reality

5G's increased bandwidth and low latency (processing data with minimal delay), will make immersive AR, which blends digital imagery with real-world environments, a reality. With expected improvements in 3D imaging, your face and body can be digitized in seconds and beamed anywhere. Think Pokemon Go, but with Star Trek-style holograms of real people you can invite to concerts or the beach.

(Even Faster) Communications

Real-time language translation, another bandwidth-intensive task, will make video chatting with family in the old country a lot easier. With faster connections that allow data processing in the cloud, instant translations of foreign languages can appear on a screen or be spoken aloud. You can potentially converse with individuals in any of the world's 6,500 languages.

Internet of Things

People will be more connected, but so will devices. The Internet of Things (IoT)—digital assistants, vending machines, wearables, and other electronics that connect to the Internet and share data—is expected to grow from 23 billion devices in 2018 to 75 billion in 2025. Enhanced data-sharing can benefit consumers (e.g. making homes energy efficient or pinging smartphones with coupons while shopping).

But experts say 5G may bring new privacy risks.

Location and data tracking

4G towers cover a mile-wide range, but 5G architecture may require towers every few blocks in some areas. The smaller the range, the more precisely individuals can be tracked. Cell phone carriers have already been shown to abuse location data, so acquiring more accurate data may increase this risk.

Also, with increased data in the IoT, advertisers will be able to learn more about personal preferences and habits.

Hacking

The IoT will increase the number of entry points for hackers, a significant threat with hackers already deploying malware that has compromised security cameras and baby monitors.

Additionally, researchers say 5G networks currently share some vulnerabilities with 4G networks, including loopholes that allow hackers to track a phone's location and use devices that can pose as cell towers to intercept calls and texts.

Western governments have expressed concerns that many new 5G infrastructures are run by Chinese companies that are legally obligated to cooperate with the Chinese government, creating a further risk to identity and privacy.

Deepfakes

Digitally manipulated videos that can superimpose an individual's face onto another body, known as deepfakes, are a particularly sinister threat. 5G could provide the bandwidth and cloud processing power for realistic-looking manipulations to occur in real-time, fooling people into thinking they are talking with trusted associates.

A great deal will change in personal communications in the years ahead. But whatever the 5G future holds, consumers must remain vigilant in safeguarding personal information.



Live-stream Leaks: Real-Time Video Can Reveal Location, Private Information

Live-streaming or "Going Live" has become a popular mode of communication, and even an established social norm for younger users. Live-streaming consists of real-time video broadcast to a public audience online using a laptop, smartphone, or tablet. It serves as an easy and versatile format for people to creatively make and share content online.

Live-streaming can inadvertently disclose a wealth of personal information to an uncontrollable public audience

Much like older communication modes such as photo-sharing, live-streaming can be incredibly compelling, and even addictive. A single user streaming a pop star's concert performance or an expert video game exploit can reach millions of viewers within a few minutes, eliciting instantaneous audience reactions in the form of comments, reactions, and likes.

Users can live-stream through broader social media services or through dedicated services. Facebook Live and Instagram Live are added features within each social media platform, alongside traditional posting, photo-sharing, and messaging components. In contrast, Periscope and Twitch are exclusive live-streaming services with specialized content focuses—specifically

video exploration and broadcasting for Periscope, and video games for Twitch.

While highly entertaining and gratifying, live-streaming can inadvertently disclose a wealth of personal information to an uncontrollable public audience, particularly when streamers document their daily lives. For example,

live content may capture a child's face and voice, the layout of the family home, and identifying information such as an address or the names of younger siblings. Streamed content can be recorded and re-shared without the creator's knowledge or approval. The public nature of live-streaming also invites contact from strangers, including potential online predators or bullies.

Using online best practices can help mitigate live-streaming risks. Trade likes for enhanced privacy by streaming only to friends, rather than to the public. Use disappearing content features, such as Instagram Stories, to help ensure a live-stream is only viewable temporarily. Finally, carefully consider your intended streaming content and surroundings before hitting record.

Encryption Explained: How “Secure Apps” Protect Your Messages

What is Encryption? The process of converting information or data into a coded message, especially to prevent unauthorized access. Encryption typically occurs in transit or at rest.

Encrypting Data at Rest: Data at rest is information being stored in a fixed place (e.g., hard drive, cloud storage).

End-to-End Encryption

Protects messages in transit all the way from sender to receiver.

It ensures that information is turned into a “secret message” by its original sender (the first “end”) and decoded only by its final recipient (the second “end”).



When you send a message using an encrypted messaging service, the service wraps the message in code, scrambling it and creating an encryption key. The message can then only be unlocked by the recipient of the message.

Two vulnerable points remain: the ends (originator and receiver). Each users’ device can still be hacked to steal the cryptographic key, or someone can simply read the recipients’ decrypted messages. Even the most perfectly encrypted communication pipeline is only as secure as the mailbox on the other end.

Why is encryption important? Unencrypted data at rest can potentially be hacked or stolen. Unencrypted data in transit is vulnerable to Man-in-the-Middle Attacks, in which an attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other.

A Traveler’s Guide to Cyber Security



Travel brings new discoveries and adventures, but what happens when you want to stay connected abroad? Ensuring the safety and security of your devices and information should be a top priority in determining how you stay in touch. Follow the best practices outlined below to limit security risks.

Before Traveling

While many people consider how to pack clothing, how you pack your electronic devices is also pertinent. Prior to departure, back up important information to a secure location, such as an encrypted external hard drive or cloud storage account.

Bring the bare minimum of devices based on the purpose of your trip. If traveling for business, you may need a laptop, or otherwise a smartphone should suffice. Consider using a spare smartphone instead of your primary. Whatever you bring, always pack your devices in a carry-on.

While Traveling

Smartphone apps such as WhatsApp, Facebook Messenger, and Skype allow for easier communication abroad with almost no extra user fees, but they contain added inconveniences and risks stemming from mobile network and Wi-Fi connectivity. Remember that mobile network data can be subject to mass surveillance in other countries. Users may also incur extra usage fees, depending on coverage and data plans.

Wi-Fi provides an alternative, but connecting your personal devices to unsecured Wi-Fi networks leaves your sensitive information—such as passwords—vulnerable. If using mobile data is impossible and connecting to public Wi-Fi is necessary, do not access sensitive personal data such as bank accounts. Run device security scans regularly to lower the risk of bringing home unwanted malware.

Arriving Home

After returning, assume your device may be compromised. Run a final security scan to check for malware prior to reconnecting to any home networks, and update passwords for your important accounts.

Last Word



We all cherish the ability to feel more connected to our families and friends. We use a growing ecosystem of devices and apps to erase long distances and share experiences in real-time—live-streaming a school play a relative cannot attend or sharing our real-time location so friends can virtually follow along on a road trip. But the desire for connection should not trump the need to keep our personal information secure. Always remember: if our friends can keep tabs on us, so can the apps they use. Limit the PII you share online, manage app settings to control data exposure, and, whenever possible, use end-to-end encrypted messaging and video chat apps to keep communications private. When 5G Internet arrives, be just as discerning with whom you connect online. Even better: occasionally put all of the devices down for a bit and opt for more real-life, face-to-face interaction.

Test Your Digital Communications Savvy: Can You Keep in Touch Safely?

1. Which of the following messaging apps uses end-to-end encryption?
a. Signal
b. Google Hangouts
c. Facebook Messenger
d. WeChat
2. What has contributed to the fragmentation of messaging apps?
a. Users mainly use messaging platforms to maintain and strengthen existing social connections
b. Pain of switching is high
c. Users simply select and download messaging services that friends and family use
d. All of the above
3. Which of the following are considered safe communication habits?
a. Don't needlessly overshare
b. Delete conversation histories when you conclude a correspondence, or at regular intervals
c. Install and run antivirus software
d. Consider your environment and ensure you're not disclosing sensitive information at home, work, or in other private settings
e. All of the above
4. The average mobile data traffic generated globally in 2018 is _____ and is expected to reach _____ in 2020.
a. 19 million terabytes per month; 7.75 billion
b. 19 trillion gigabytes per week; 775 billion
c. 19 billion gigabytes per month; 77.5 million
d. 19 billion gigabytes per month; 77.5 billion
5. Which of the following is NOT a safe option when communicating while traveling?
a. Pack electronic devices in carry on
b. Back up important information on an encrypted hard drive
c. Access public Wi-Fi whenever possible to stay connected
d. Run a security scan after arriving home
6. What are the risks of 5G?
a. Faster communications
b. Augmented reality
c. Location- and data-tracking
d. All of the above
7. What is a Man in the Middle Attack?
a. A man attacks two people by standing in the middle of them
b. An attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other.
c. An attacker openly relays and alters the communication between two parties who believe they are directly communicating with each other.
d. All of the above
8. How many points of vulnerability are there when using encrypted communications?
a. 5
b. 2
c. 0
d. 1
9. What are considered analog communication methods?
a. Landline telephones
b. Handwritten letters
c. Early fax machines
d. All of the above
10. When was the rise of mass Wi-Fi?
a. 1990s
b. Late 2000s
c. Early 2000s
d. 2015

In the Next Issue

Are intelligent personal assistants (IPAs) getting too smart?

We no longer just ask Siri or Alexa random trivia questions. We expect them to perform chores, such as booking restaurant reservations, and, using artificial intelligence, complete tasks without being asked (e.g., scanning email and adding new appointments to our calendars). For that convenience, the ever-listening microphones are always near, and consumers grant them access to vast amounts of personal data, including location, calendars, email, contacts, and online search histories. The summer issue of CPIQ will explore how IPAs are used in our daily lives, the potential for hacking and data misuse, and how consumers can protect their privacy from IPAs that eavesdrop or misbehave.



For more detailed information on protecting and managing other key elements of your identity footprint online please check out the:

IDENTITY AWARENESS, PROTECTION, AND MANAGEMENT GUIDE

A GUIDE FOR ONLINE PRIVACY AND SECURITY COMPRISED OF THE
COMPLETE COLLECTION OF DEPARTMENT OF DEFENSE SMART CARDS
EIGHTH EDITION, MARCH 2019



BROUGHT TO YOU BY:



U.S. DEPARTMENT OF DEFENSE

IDENTITY AWARENESS, PROTECTION AND MANAGEMENT GUIDE