Managing Your Digital Life

A consumer's guide to cybersecurity

Interactive Table:
Click to Jump to Page.

CONTENTS

Simplify and Protect Your Digital Life

What is our digital life? Our digital life is how we've adopted technology to manage the various components of our life, from our professional lives to our personal lives and everything in between. It's how we integrate and interact with technology to maximize our experiences.

However, as we more deeply adopt technology into our daily life, **we also introduce significant cybersecurity threats and risks.** These risks are inherent; they come alongside the technology that we choose to adopt and use. The threats and risks are real. They seek to hijack our lives—be it the technology itself for malicious intentions or, as a result, the threats also create inconvenient disruptions and sometimes destructive consequences in our daily lives. These malicious activities are allowed to go unchecked because technology is so commonplace in our lives. In other words, we have become so comfortable with the presence of technology and so accustomed to its functions and benefits that we don't always consider the negative impact of the threats and risks associated with our digital life.

There are several considerations to be made regarding our digital life. The first consideration is all about what: What technology are we going to use daily? Part of this question is answered for us depending on our professional environment. There's not a professional setting today that doesn't require the use of some technology such as a computer or mobile device, software, or communications applications that allow us to interact with people in our professional environment and circle of influence. Mobile devices—the foundation of our digital life—have evolved to such a mainstay that it is nearly impossible to navigate life without one.

> "Mobile devices—the foundation of our digital life—have evolved to such a mainstay that it is nearly impossible to navigate life without one."

The second consideration is all about how: How will you use technology in your daily life? This is particularly driven by mobile devices, as they have become incredibly multifunctional, meaning they can be used to facilitate nearly any need arising from any component of our digital life. How we use technology has almost become second nature, depending on the need.

Here's a few examples:

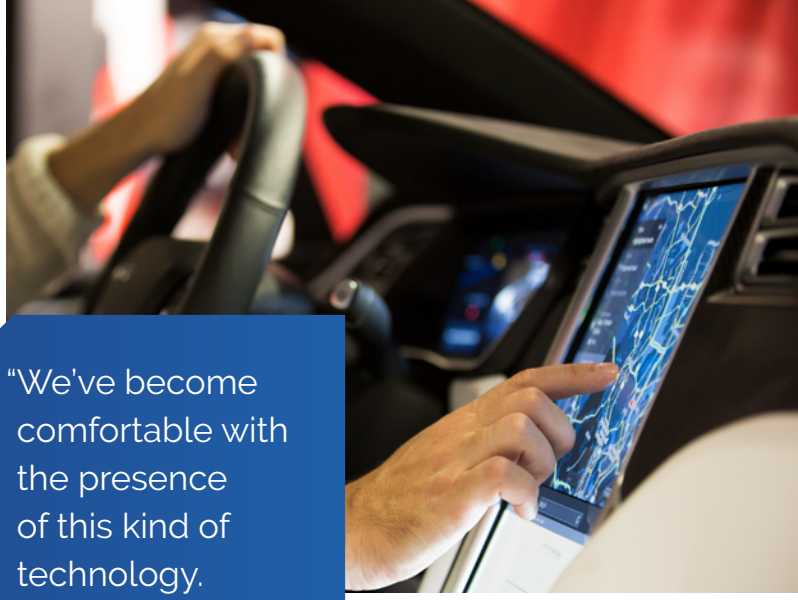
If you're traveling from one place to another and you're not familiar with the directions or how to get there, you're typically going to pull up your GPS application on your mobile device, punch in the address, and have it guide you to your destination.

People don't really remember telephone numbers anymore. Instead, to connect with one another, we rely on those numbers being programmed into our phone. Give it a try—could you recite the telephone number for a particular individual without checking your phone? Gone are the days of memorizing telephone numbers, an act that is now completely facilitated by the mobile device.

What about the precious memories we desire to capture from a gathering, event, or trip? We used to use a stand-alone camera to capture these moments, whether it was a 35mm or a Polaroid. Now, we simply pull out our mobile device to capture our important moments, which are then stored digitally on your mobile device or in the cloud for quick and easy sharing with anyone on the face of the planet.

These are all instances of how technology can quickly facilitate a need that we have in our daily life, and there are so many more examples out there.

We've become comfortable with the presence of this kind of technology. But we've also become relaxed about recognizing the potentially negative impacts it can have on our lives. These technologies are information treasure troves. As a result, this information acts as a personal footprint for the owner of the technology, one that captures a story about who this person is. There can be great benefit to this—but also great challenges, because while the information can be used for legitimate and benign purposes, it can also be used for malicious purposes and nefarious gain.



"We've become comfortable with the presence of this kind of technology. But we've also become relaxed about recognizing the potentially negative impacts it can have on our lives."

Your Digital Life Etiquette

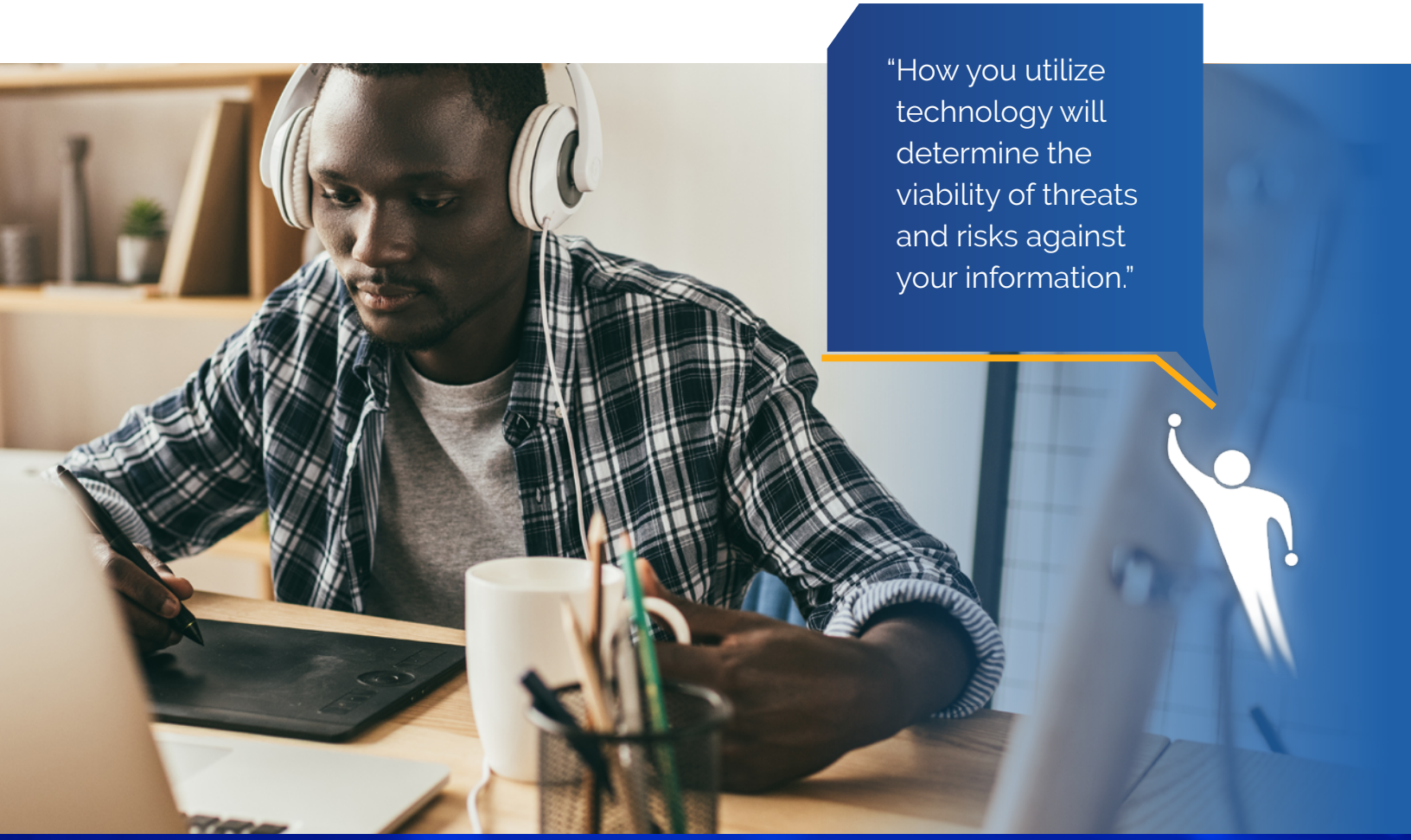
To minimize the risk of malicious actors gaining access to our digital life, we need to adopt a "digital life etiquette" that makes it challenging to not only gain access to our digital life but also to navigate it in any way. This digital life etiquette is a behavior-based recommendation for managing our daily digital lives. Again, it all comes back to how: How you utilize technology will determine the viability of threats and risks against your information, as well as the resources that are connected to your daily digital life.

To understand the appropriate digital life etiquette, we must first understand what our digital life is made up of. The goal is to minimize the risks associated with having this technology in our lives in the first place. Our digital life is made up of technology components that enable us to better manage the various functions of our life, which consist of the following:

Mobile devices such as mobile phones, tablets, smartwatches, laptops, and any internet enabled device.

Online accounts across all sectors and services, including banking, retail, travel, e-mail, streaming entertainment, and all accounts that allow us to interact with businesses or people online.

Software such as Microsoft 365, Google Apps, gaming apps, productivity apps, and entertainment apps like iTunes.



Here's the digital life etiquette bottom-line:
The behaviors we engage in while using these services and technologies will determine how secure or insecure we are to the rest of the world. The behaviors we engage in are driven by what we are most comfortable with. This comfort level stems from habits and patterns we develop over time; the culture in which we were introduced to the technology; and the reasons why we've elected to keep using it. Over time, as we engage in and interact with technology, we develop a comfort level that typically does not include mindfulness of safety and security. As a result, we unintentionally create numerous constructs in our digital life based on our behaviors. This creates vulnerabilities that can be exploited by malicious actors who also understand how these behaviors translate to weak and vulnerable constructs.

What are the reasons for these weak and vulnerable constructs? First, as our digital lives evolve and explode, so, too, has the tediousness of managing our digital life, driven by the sheer amount of information that we must remember and manage daily. It creates challenges around managing this information appropriately. As a result, we develop ways of managing this information that allow us to move on with our digital life without being bogged down with having to remember all the information necessary to engage in and interact in our digital life.

> "If a hacker can obtain just one set of credentials, then we have ultimately given the hacker unfettered access into our entire digital life."

For example, on average, **each consumer maintains at least 30 to 40 different online accounts.** That's 30 to 40 different sets of credentials that a consumer must remember to access their online accounts.

And so, to manage all this information, we fall back on what's comfortable to us, what's easy for us. For example, we typically repeat the same credentials over and over. It makes sense; it's easier to remember our credentials if we use the same details. Or we write down the credentials and nonchalantly store these notes in a place where they can be readily and easily accessed. Or our credentials are made up of information that is easily known, such as birthdays, child names, street names, or relatives.

This is a problem. If a hacker can obtain just one set of credentials (and there are myriad ways that a nefarious attacker can do this), then we have ultimately given the hacker unfettered access into our entire digital life.

Organize your Online Accounts

We are creatures of habit, and we love dwelling in our comfort zones. With this in mind, I'm going to suggest some account and credential management strategies that allow us to better secure our digital life without disrupting our coveted comfort zone. These suggestions are easy to implement.

The first suggestion is to create a "bucketed" list of your online accounts. Think about all the accounts you maintain and list them out by category. You'll compartmentalize your online accounts into buckets, or what I call account categories. An account category is a delineation of accounts that are all meant to support the same purpose, such as financial accounts like credit card accounts, bank accounts, and retirement accounts.

Next, you might have travel accounts such as airline accounts, rental car accounts, and hotel rewards accounts, all meant to support the purpose of travel and leisure. In this example, "Financial" and "Travel" are what I would consider to be account categories. If you look at the 30 or 40 accounts you have, you can draw clear circles around common sets of accounts to help compartmentalize everything.

By creating lists of your online accounts, and then organizing them into 'buckets', you can set the stage for a compartmentalized approach to securing your online life.

"**Compartmentalization** is designed to create boundaries ... if a hacker gets into one category of accounts using credentials that they may have stolen from you, they can't use those same credentials to access your other account categories."

Next, create a set of credentials such as username, e-mail, and password for each account category. E-mail providers such as Google, Yahoo, and Microsoft allow you to create multiple e-mail accounts on their platforms. Some online accounts may require you to create an actual username, while other accounts may require you to use an e-mail as the account username. Regardless of the requirement, the suggestion holds, though the idea here is particularly related to online accounts that require e-mail as the username. (Internet companies want to make it easier for you to access their services and they know it's easier to remember an e-mail address than a single username that you will only use for this online account). The practical behavior we engage in is using a familiar, oft-used e-mail address along with the password. If a hacker can discover your daily e-mail address and password—and there are many ways for a hacker to do just that—then they gain the credentials for every online account for which you use these credentials.

What we want to do is compartmentalize our online account credentials. This makes it easier to manage all your credentials while making it harder for a hacker to gain access to your entire digital life. Remember, compartmentalization means defining buckets or categories of online accounts that serve a similar purpose that we can group together. Compartmentalization is designed to create boundaries around these grouped accounts. So, if a hacker gets into one category of accounts using credentials that they may have stolen from you, they can't use those same credentials to access your other account categories.

Getting Started with **Compartmentalization**

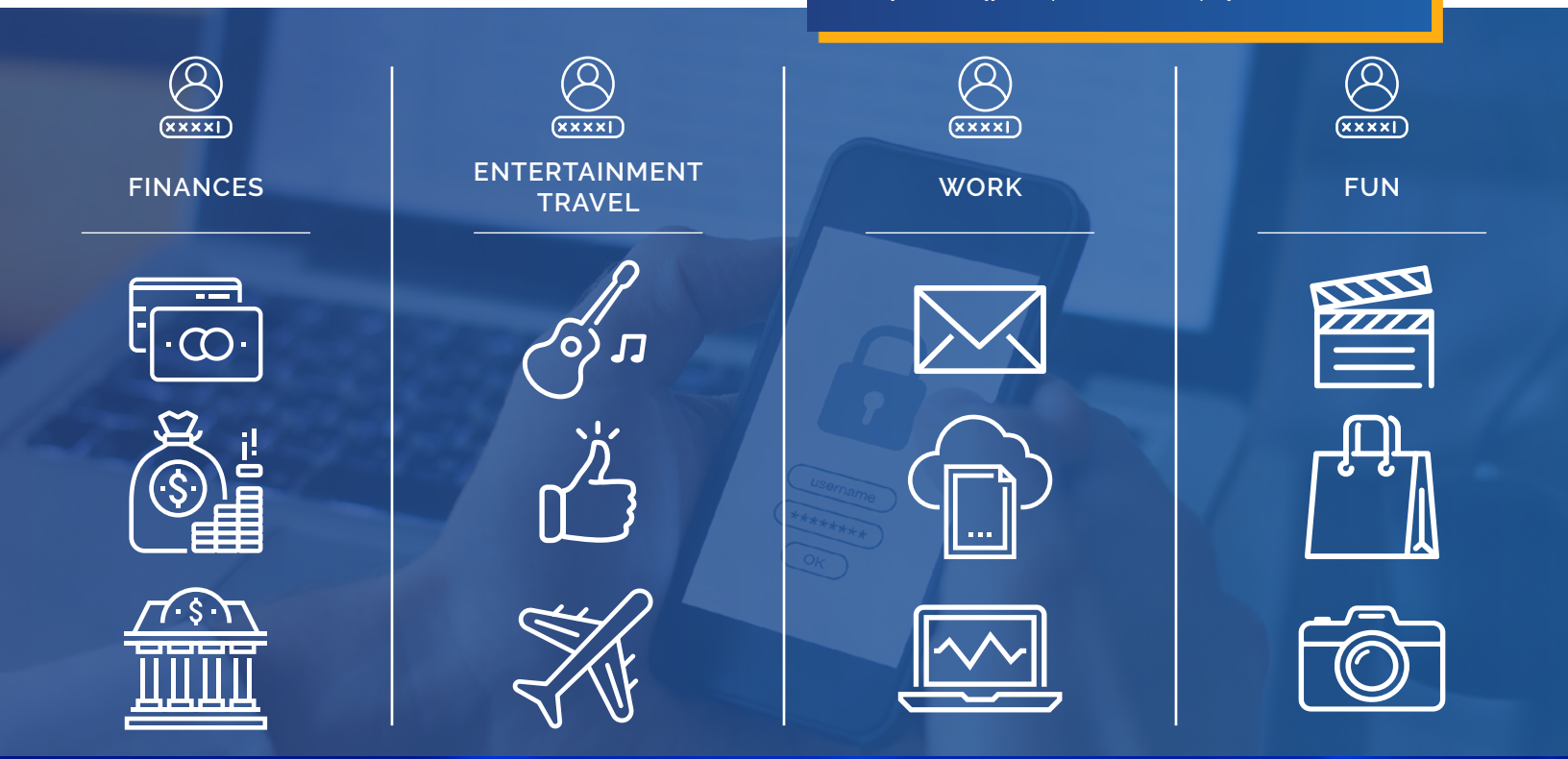
Most online accounts require an e-mail address and a password as your basic set of credentials. To begin, generate an e-mail address that you do not use for daily communication. This e-mail address should only be used as your username for your online accounts.

Create an e-mail address and password for each account category in your control (e.g., one set for Financial, one set for Travel, and so on). This way, you go from having 30 to 40 different sets of credentials down to about seven different sets of credentials. But remember: The e-mail addresses that you create should only be used for account access; they should not be used to send or receive daily e-mail. The reason for this is that the more you use this e-mail address in public, the more opportunity there is for someone with malicious intentions to discover your e-mail address and password.

You can advance this idea by altering the account category e-mail address and password for each account in a given category. But do so in a way that is easy to remember so that you don't have to write the details down. (This defeats the purpose of this process altogether!) Some might say: Well, why don't you just use a password manager like LastPass? It's OK to do this, however, you are now putting the safety and security of your digital life into the hands of another software application. It's a risk consideration. A better approach is account compartmentalization and category credentialing. It makes it easy for any consumer to manage credentials from memory without writing details down or relying on a technology to help you manage this information.

You can do this with usernames as well. Recall that some online accounts require an actual username which is not an e-mail address. Many providers will offer suggestions for usernames that you can use, or they will allow you to choose your own username. The suggestion of creating usernames for each account category still holds here.

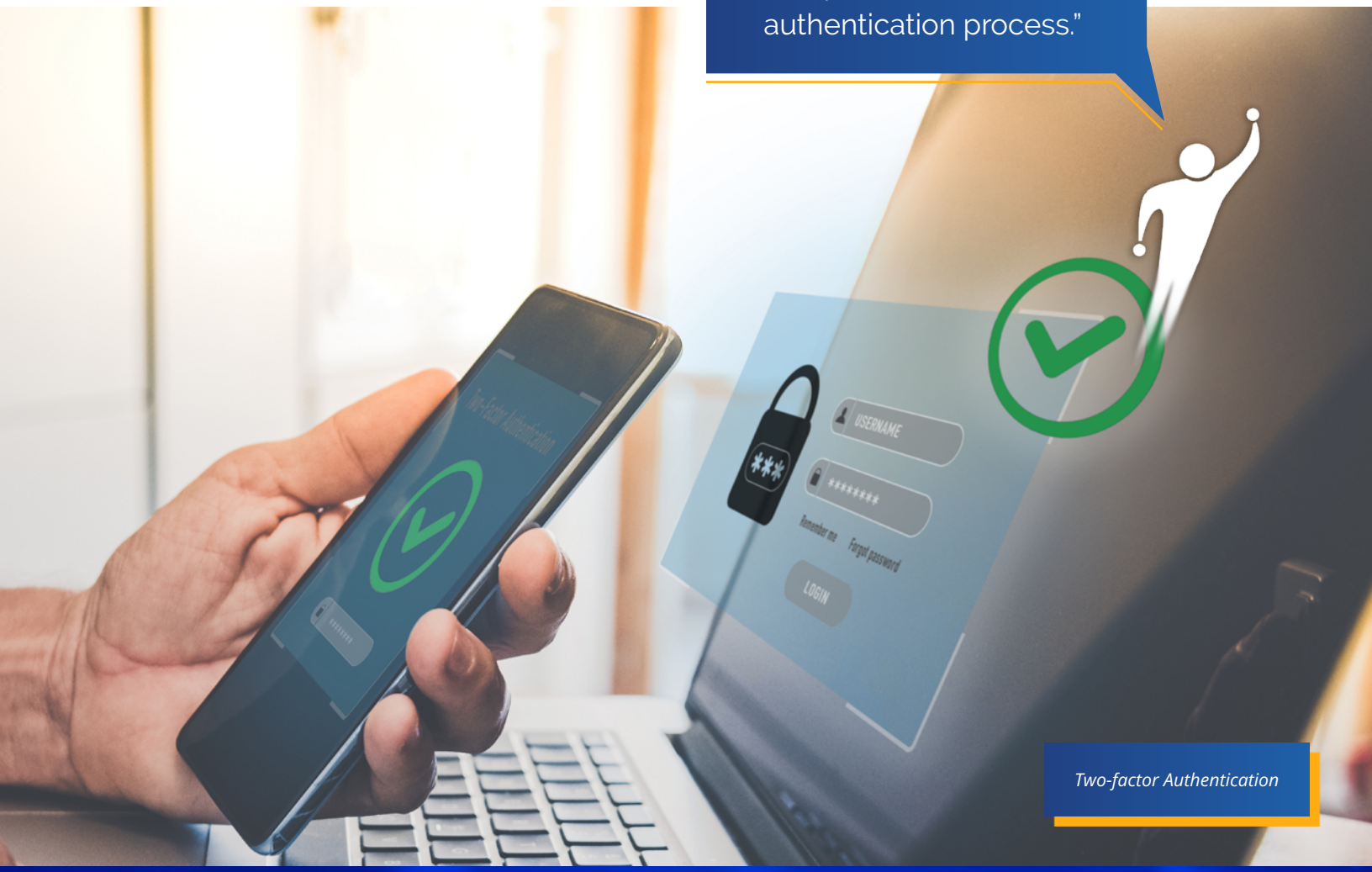
Now we start to see how our buckets are separated into categories, each with their own unique username login, and of course different passwords on top of that.



My last suggestion to improve and secure your digital life is to add an additional layer of security, wherever possible. Many popular online service providers also require multifactor authentication (MFA) to be enabled on your account, which provides an additional layer of security. Some MFA scenarios allow an e-mail account or a mobile phone as the secondary component in the authentication process. The best choice here is to use the SMS or text message function as the secondary component in the authentication process. This allows the authentication process to be facilitated by two very different technology components. So, if a hacker gains access to your e-mail account and you've set up MFA using your e-mail as the secondary component of the authentication process, then the attacker can confirm that authentication process and gain entry to the targeted online account.

Of course, you can take these suggestions and tailor them to your own needs—what I've presented here are just some simple ways that you can increase security and better manage your digital life. Are you finding it challenging to manage all your credentials across your many online accounts? Online account compartmentalization—and improved digital life etiquette—can help.

> "The best choice here is to use the SMS or text message function as the secondary component in the authentication process."



Two-factor Authentication

888.601.3064 • DATA-DEFENDERS.COM