# Best Privacy Practices In 2022
## *Part I*

*By Trey Peacock, Winning Cases Based On Science & Data For Over 25 Years*
*Originally published on LinkedIn.com*

Of the many intersections of technology and law I have written about in these articles, none is more important than privacy. Data Privacy Day is January 28 so there is no better time to discuss best practices. Technology companies, social media empires, and businesses continue to erode personal privacy protections which are further weakened by neglect and unbolstered by legislation. In addition, online crime, identity theft, and impersonation have never been more prevalent or dangerous. The weapons available to would-be hackers and thieves grow more numerous and serious by the day. Therefore, the actions you take to protect your data are more critical than ever.

In this article, I will identify the best practices that every web and technology user should employ to best protect themselves, their workplace, and their data from unwanted access, intrusion, and use. Starting with the easiest steps and moving to the most complicated, you should do your best to implement every one of these tips. But, if you cannot muster the effort to implement all of them, take care to adhere to those that are most relevant to your specific situation or usage style. With this article, I hope to provide information you can use to implement an ample defense against online mischief, and to imbue in you a sense of confidence and competence about your online security.

**Don't Reuse Passwords**

I begin with the most basic tenet of online privacy: do not re-use your passwords. Ever. Just don't do it. Every time you re-use the same password across another platform or login, you multiply the chances that it will be leaked, stolen, or otherwise obtained for undesirable use. Additionally, if that password falls into the wrong hands, you have once again multiplied your exposure, as

a re-used password grants access to multiple accounts on multiple platforms. And bad actors know which sites to start with when testing a password to determine whether it has been re-used. Limiting this risk is one of the easiest and most effective ways to safeguard your information online. If you have trouble remembering a whole slew of unique passwords, the next tip is just for you.

**Use A Reputable Password Manager**

Instead of relying on your memory, a word doc on your computer, or – heaven forbid – a sticky note on your desk, use a reputable password manager to create and store the unique and complex passwords and account usernames you have created. My longtime recommendation, Dashlane, has extended functionality that safely stores all passwords, suggests a unique and complex password when creating a new account, and even supports the use of MultiFactor Authentication codes without leaving the app. Employing Dashlane or a similar product such as 1Password adds a very important second layer of protection to any password or account, so long as your Master Password is secure, not recorded anywhere online, and, above all, unique. Additionally, password managers boost the integrity of every password on your account by preventing you from forgetting a complex password and replacing it with a simple one that may or may not have been used before (or is easy to crack). Though these services usually cost a small amount of money (most often a monthly on annual subscription cost), the expense is well worth the added security benefits and peace of mind.

**Use A Complex Device Passcode**

Although TouchID and FaceID have been very well-integrated into the latest suites of smart mobile devices, all iOS and android phones and tablets occasionally require input of the device password, such as when a user is wearing a face mask or restarting a device. In these cases, a four or six-digit numeric passcode does not provide a sufficient level of security, especially because your mobile device usually houses some of the most sensitive and important pieces of information in your entire digital portfolio. A four-digit passcode containing only numbers has 10,000 possible combinations. By using an alphanumeric passcode with 8 characters or more, you astronomically increase the security of your passcode. By choosing from both numbers and letters, you explode the number of potential combinations from 10,000 to nearly 3 trillion. Upgrading your passcode is a no-brainer. Lose the 4 digit passcode (that might also be your partner's birthday or your ATM PIN), and go for something a bit more secure to protect all those private documents, texts, and apps that you hold so dear.

**Regularly Use a VPN**

Now that we have covered the most basic ways to maintain your digital privacy, let's move into some of the more complicated but no less crucial practices that will greatly improve the security of your online footprint. Your documents and accounts are not the only potential target for scammers, hackers, or other bad actors. Your browsing activity can be just as revealing, and potentially even more lucrative for would-be data miners who can use your information, either to pinpoint your identity as part of a larger plan or scheme, or to gather and re-sell your information to others. The most simple and reliable way to protect your browsing activity is to regularly employ the use of a VPN, or Virtual Private Network on your computers, phone, and tablets. These

programs route your network traffic to a series of nodes in other locations across the globe to mask your true location as well as nest your actual activity within an encrypted tunnel, greatly impeding others from accessing and mining your information as it bounces between your machine and the network nodes. Feel free to take a deeper dive on the VPNs I recommend in this article.

**Opt Out of Data Collection**

One of the most useful and impactful new features in iOS 15 is the ability to choose when certain apps track your data and send it along to the developers for use as they see fit. Apple has added a feature that, upon opening a given app, prompts the user to opt in or out of data gathering. To be clear: you should opt out of these situations whenever possible. (Step-by-step instructions on doing this can be found in my previous article). There are very few benefits to sharing data with apps and companies, and very many drawbacks to doing so. When in doubt, always remember the mantra: "If the service is free, you are the product."

**Avoid Scams**

Another crucial element of maintaining your own network security is training your instincts and eye to avoid intrusive scam and data mining attempts. These scams can take many forms and entrap even typically vigilant and careful victims. Some masquerade as robocalls inquiring about your "vehicle warranty" or your "software license" and will ask you to reveal sensitive personal information over the phone. Others take the form of an innocuous email with a hyperlink that, once clinked, will install a nefarious piece of spyware or ransomware that turns your own device into an instrument of observation and extortion. To avoid these scams, maintain discipline in your interaction with all potential sources. Never click on hyperlinks you do not recognize. Ignore and delete emails and text messages that appear to be phishing. Carefully check the actual email address of a sender as many will change just a single digit of a legitimate email address. Remember that banks, investment firms and many other institutions make clear they will never ask you to enter your username or password by email. And never give out sensitive information over the phone, unless you dialed the organization yourself and are confident you are communicating with the intended entity or person.

**Be Careful With Money Transfers**

Finally, be extremely careful and judicious about to whom you send money and how. Though personal wire transfers are not as commonplace as they once were due to modern money transfer apps (covered in a previous article), you should take care with all methods of sending and receiving money, as they are targets for some of the trickiest scams that exist these days. A common scenario involves receiving a mysterious payment that another user will claim that they sent you "by accident," and ask you to send it back to them. Do not fall for this. Almost always, the unseen truth is that the original payment was sent via a method that will bounce, leaving you without both the money you transferred and the money you believed you received. Additionally, when using bank wire transfers, always confirm the account instructions verbally or over the phone with a person you know to confirm the account instructions for where you are sending a payment. There are frequent instances of scammers impersonating family members and friends and even intercepting emails and pretending to be a party you regularly deal with in order to solicit "emergency" payments or changes in account information. Once you provide them with

information, they use it use to rob you. Employing these practices will help safeguard you against all manner of online payment scams.

Though collectively these practices may seem paranoid, cynical, overly cautious, or just plain difficult and boring, employing even some of them (but hopefully all) will go a long way toward improving your online security. These protections may even keep you from falling victim to a scam that could cause great personal, digital, or financial harm. Keep all of these tips in mind as you continue to expand and develop your online footprint, and you will be well guarded against even the most intrepid hackers. No thanks necessary--just keep reading these articles.

Stay tuned for our second part of this article next month which will take you step-by-step through implementing some of these privacy practices on your own social media and other frequently used accounts and devices.

## About the Author

*Trey Peacock, a partner at Susman Godfrey, has been winning cases based on science and data for over 25 years. He has also chaired the firm's IT committee for over two decades. Learn more about Trey here.*