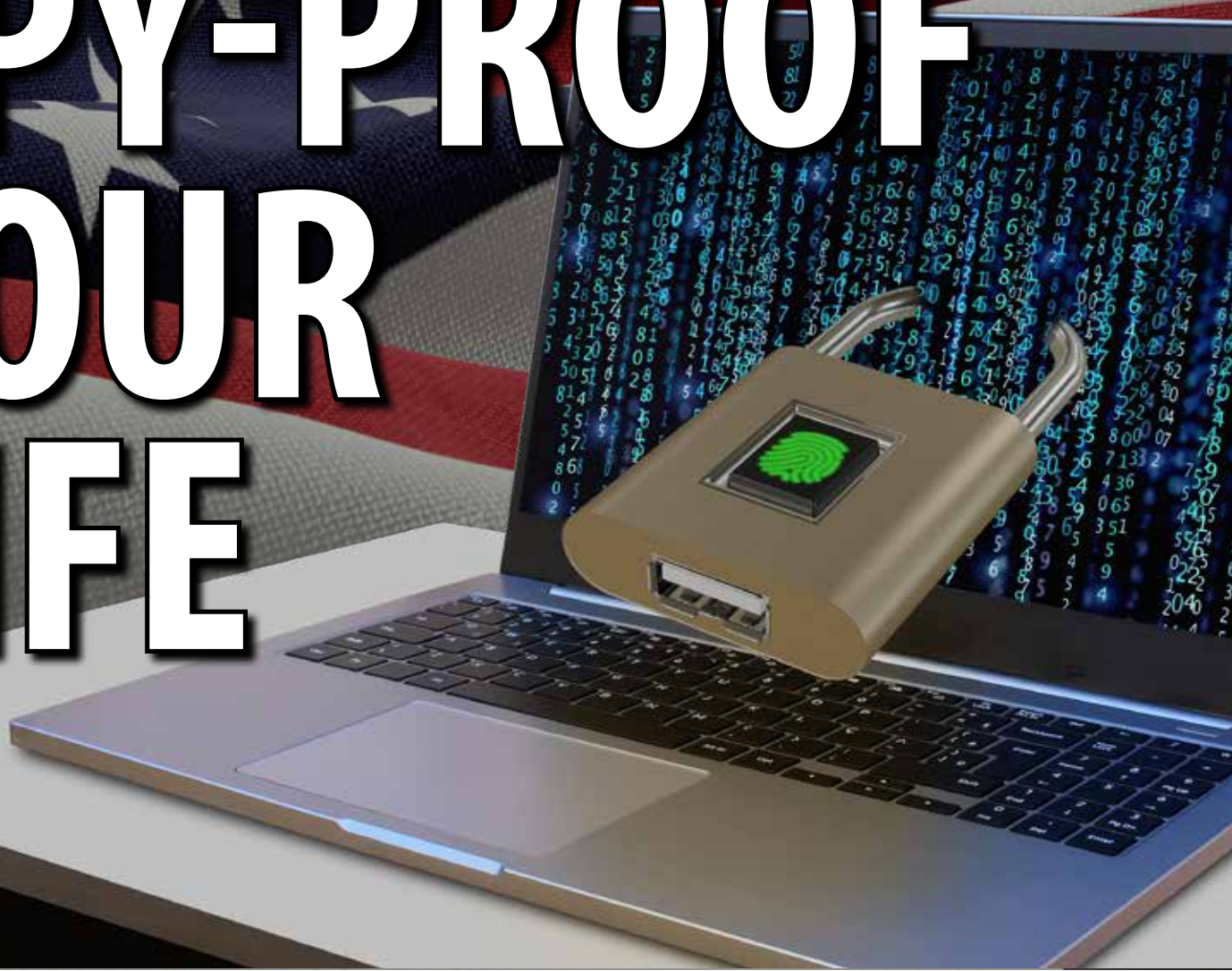


CHECKMATE



**SPY-PROOF
YOUR
LIFE**



**BUILD YOUR PERSONAL DIGITAL
FORT KNOX**

Prepared By Ian King and Michael Carr

Checkmate: Spy-Proof Your Life

Build Your Personal Digital Fort Knox

By Ian King, Editor, *Strategic Fortunes*

IN today's tech-driven world, where social media platforms like Meta, Instagram — and TikTok *especially* exist, your private information is always a click or swipe away from being compromised.

And if you actually use TikTok, you'll find just how little privacy you truly have.

A quick web search will detail all the information you need to relinquish to use the full range of features on the popular app.

According to TikTok's website, it collects:

- Your browsing history, including the videos you watch.
- Your private messages, including the comments you compose, send *and* receive in the app.
- Purchase information, including payment card numbers or other third-party data, billing and shipping addresses.
- Information you share through surveys, your participation in those ever-so-popular challenges, research, promotions, marketing campaigns, events or contests such as your gender, age, likeness and preferences.

And, of course, all this (and more), in addition to the usual — name and email address — are a *major* privacy and security concern for many Americans.

In fact, laws are being made across America banning TikTok for use by federal employees as you read this.

Recently, Montana became the first state to ban TikTok altogether, effective January 1, 2024.

It has also already been banned for state employees in 34 U.S. states.

But these concerns don't just start and stop at TikTok. In today's tech-driven society, privacy and security concerns sweep the nation as many of us navigate this duality of the real world and the digital.

Another common knowledge Trojan horse is drones.

Of the 900,000 commercial drones in the United States, half — 450,000 — come from one place.

DJI.

A Chinese company that's been the welcome benefactor of massive funding from President Xi's communist government.

Today, DJI is on just about every banned list you can think of and has been classified as a threat to national security.

DJI maintains access and control over the data captured by each of its drones ... GPS coordinates, footage and facial recognition technology.

With very little effort — a simple software upgrade — DJI can take over any drone they want or a bunch of them.

So there's a simple solution: Don't use TikTok and don't buy a DJI drone.

Those are easy.

But there are more steps you can take today. Because remember, nearly everything we do today is online, which is essentially a hacker's playground.

Email...

Google...

Online retail and grocery shopping...

Digital wallets...

Even online banking.

Private companies store your information on servers that can be hacked. Websites you visit are tracking every "step" of your digital footprint and passing that information on for profit.

Even ATMs can be compromised by hackers looking to steal information from the magnetic stripes on the back of your bank card.

Your personal information is just as valuable as your home, cars and the gains in your investment portfolio — if not more.

In fact, without being able to verify your personal information, you can't buy a new car, home, or even open an IRA.

And if you aren't safeguarding your most sensitive information, you're at risk of it landing in the hands of the wrong person — so you need to ensure it is secure.

So in this report, I'll break down four phases to consider when securing your private information.

Phase 1: 4 Steps to Secure Your Private Information

When it comes to your personal information, you have to view it as equally as important as any physical asset.

Securing your privacy is not impossible. Celebrities and other "high profile" individuals do it all the time — and so can you.

Much of our most protected or "discreet" information is typically housed passively.

The birth certificate in the manila folder underneath your mattress ... the medical file saved to your work computer's hard drive ... the online banking window that you always close but never log out of — all things that *should* be protected — but often aren't.

Some of our most sensitive information is sporadically placed in random — *often unsecured* — locations throughout our lives, leaving it unprotected.

So the first step to changing that requires a more introspective approach.

It requires you to do a self-assessment to determine what qualifies as private — or "compromising" — information.

For me, this is any information that could be stolen or hacked (i.e., checking, savings and other finance-related accounts, social security number, emails, medical records, etc.).

Next, you'll need to assess *who* has that information. Is this private information that you've shared over email at some point? Have you misplaced these documents or are they stored in a shared personal or work computer?

Ask yourself:

- **What information do I need to protect?**

Again, this would include any information that could potentially be compromised in a way where your assets or identity could be stolen or your personal accounts be hacked (PC, phone, passwords, medical records, contact lists, banking information, etc.).

Step 1: Compile a list of sensitive information about you and your dependents, where it's kept, who has access to it and what is stopping others from accessing it.

- **Who do you want to protect it from?**

Any person or entity that could pose a threat to your privacy, assets or personal information. This includes business partners, national or foreign governments, hackers and scammers — all of which can have different motives and different methods of attack.

Step 2: Make a realistic list of who might want to gain access to your private information and what they might want to do with it.

- **Determine the threats versus the risks.**

A threat is a bad thing that could happen, whereas a risk is the *likelihood* that it will.

For example, no matter where you live in the U.S., there is always the threat that floods might damage your home. However, the risks of that happening are far greater in South Florida than in Nevada. That same logic could be applied to your private assets.

Your mobile phone provider can access all of your phone records and use that data against you. While your mobile phone provider has the capability to access your data, the risk of them doing so for any purpose that could harm you is low.

On the other hand, if you know you are the target of an investigation by legal authorities or a litigant, you might be concerned that they would try to obtain your phone records with a court warrant. That would dramatically increase the risk of your mobile provider's data threat.

Similarly, sending a text to your spouse over an open Wi-Fi network poses less of a threat to your personal information than emailing your attorney over a legal matter.

Step 3: Survey your personal affairs to see where you are at the greatest risk of a privacy breach and prioritize securing those assets.

- **What are the consequences of not protecting this information?**

When you identify threats and their likelihood of happening, you also want to identify the costs to you *if* they happen.

Step 4: Rank the risks to your privacy assets that you identified in Step 3 from most to least consequential, or essential, optional and nonessential/chance.

Determining threats versus risks is a personal and subjective process. What some find to be a threat could be a risk to others, so it's important to determine what these things mean to you.

Assessing and ranking this information lets you immediately see which threats you should address and in what order: Start with the most consequential threats in the "essential" bucket and work your way down.

Once finished, these four steps will be your launchpad to categorize and secure your most private information.

Finally, never fill in unnecessary or optional information in online forms. Use made-up details unless it is absolutely necessary to provide accurate information.

Phase 2: Armor Yourself Against the Threat of a Hack Attack!

Now, I've briefly touched on the potential threats of social media and the risks of other companies and entities having access to your data beyond your control.

Meta, Google, credit bureaus (Experian, Equifax and TransUnion), hospital groups, Amazon and Walmart are examples of companies that maintain highly detailed files about you. In most cases, we offer them this information voluntarily in exchange for a service that we get for free (i.e., Facebook).

However, make no mistake — these companies collect *huge* amounts of information about you and centralize it on massive servers, where it can be analyzed, manipulated and used to target you for advertising. It can even be sold to third parties for that purpose.

Even if the companies give us an “opt-out” option, their access to this information puts you at risk. Because even if the companies agree not to use your information in some way, they remain vulnerable to being hacked by those who will.

Take the 2017 hacking of Equifax, for example. Hackers managed to get into the company’s consumer database for several months before they were even discovered. Information about more than 140 million Americans, including name, date of birth, address and social security number, was stolen and leaked.

That’s essentially all the information someone would need to commit identity theft or fraud against you. So here are a few things you can do to combat this:

- **No. 1:** Consider whether getting on to a company’s database makes sense. Once you’re on, that’s it. Even if you manage to get a company to delete your information, there’s no guarantee that it hasn’t already been hacked or that it might be stored in a way that would allow it to be recovered.
- **No. 2:** Open an account with a credit-monitoring service that will alert you of any changes to your credit reports, including new account openings. It’s not necessary to pay for expensive subscription services anymore. Most of the major credit bureaus offer credit-monitoring services.

Third-party websites like www.Credit.com and www.CreditKarma.com also offer quick notifications of any activity on your credit record. These companies make money by channeling credit offers to you, but I believe it’s worth it.

- **No. 3:** A credit freeze. That’s when you tell a credit bureau not to release any information about you to anybody trying to obtain your credit report. For example, if somebody tries to open a credit card account in your name and you have a credit freeze active, they won’t be able to do it. And you’ll get a notification that someone tried. The major downside is that you have to remember to unfreeze your credit record before doing any business that would require a credit poll.
- **No. 4:** Use two-step authentication for everything. Two-step authentication is basically a process where in addition to entering a username and password, you also have to enter a one-time code that is sent by email, text, or some other means before you’re allowed to log into a service. This is especially important for any crypto exchange (like Coinbase) where someone could log in and steal your crypto.
- **No. 5:** Sign up to receive any notifications that an online company may offer. Whether it’s deposits, withdrawals, account modifications or name changes — you’ll receive a notification about *anything* that happens on your account. The quicker you learn about something you *didn’t* do, the quicker you can act.

With that, I highly encourage you to take the above precautions when protecting your private information. Because once the sort of data Equifax, TikTok or Meta has from you is compromised, that’s it.

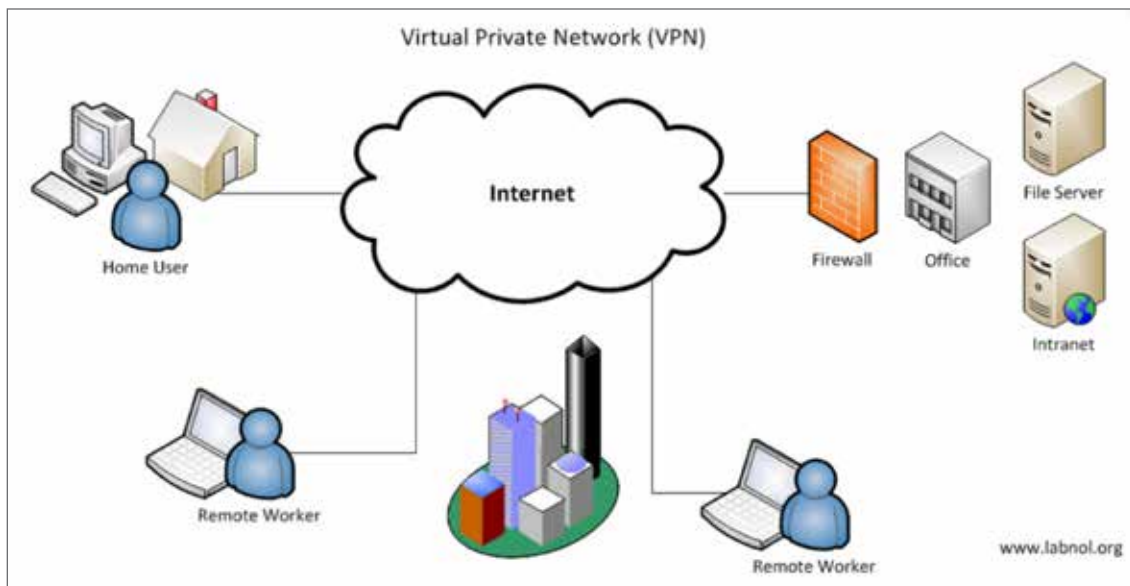
There’s no putting the toothpaste back inside the tube. The damage has already been done.

Phase 3: Spy-Proofing Your Web Browser Using VPNs & Cloud Storage

As I mentioned, the internet is a hacker’s playground, so protecting your internet connection and privacy online is critical.

This can be as simple as using password-protected wireless internet in your home and office — or unplugging your webcam and microphone when not in use.

Or it could be the best and slightly more complicated option — a *virtual private network (VPN)*.



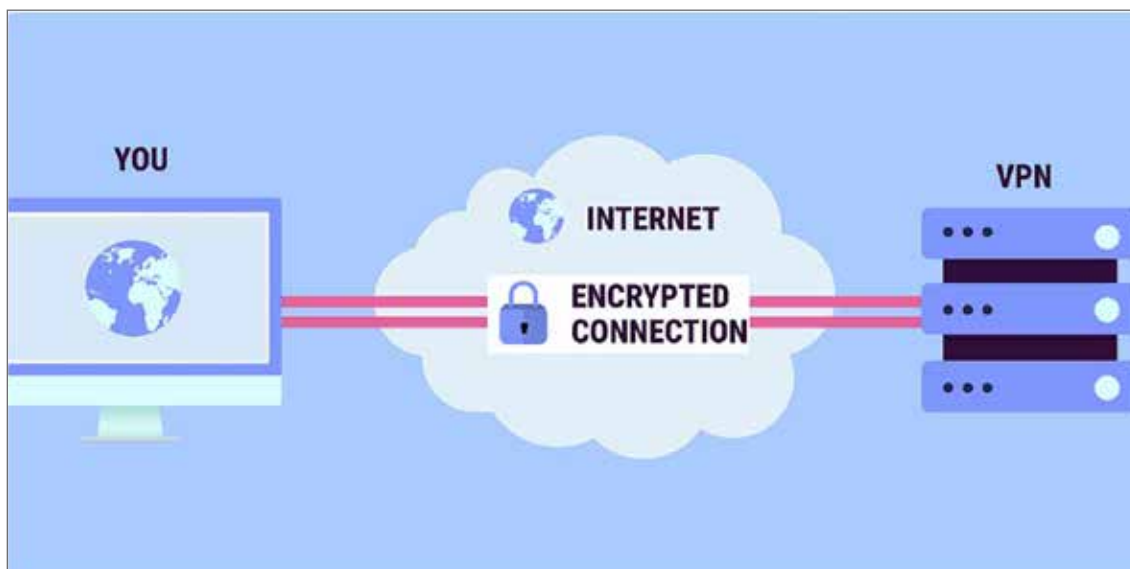
A VPN creates an encrypted private network for you across the internet. VPNs allow a computer or network-enabled smartphone to send and receive data across the internet as if directly connected to whatever is on the other end — including websites you visit.

When you use a VPN, all the IP addresses of the computers connected are hidden from outsiders, and data sent between them is encrypted.

So while the VPN uses the public internet, it is *completely* invisible to those without the right credentials.

For example, if you connect to a website using a VPN, your computer's location and other personal data are invisible and anonymous, as is anything you do on that website.

You could set up a VPN on your computer or phone by installing software that converts your internet traffic into a password-protected encrypted form. You use the same browser you normally do, such as Google Chrome or Firefox.



Most people use paid services (\$5 to \$20 per month) that host the VPN for you. However, you'll want to ensure that they do not store usage logs of your internet activity on their servers, as it can potentially be compromised.

I've listed several quality VPN services for home users below:

- [NordVPN](#) is highly ranked for privacy and works on Windows, Mac, iPhone and Android phones with a single account. It is highly customizable and allows you to shop around for the fastest servers.
- [ExpressVPN](#) is based in the British Virgin Islands and is one of the most popular and successful VPN providers. It's an advocate for internet privacy rights and has a high-speed network of servers across 94 countries and easy-to-use platform for many phones and operating systems. *ExpressVPN keeps no usage logs.*
- [IPVanish](#) has servers in more than 70 countries, keeps no logs and accepts bitcoin. It's a good low-cost provider, recommended if you want a solution that delivers uncompromised security and speeds.
- [VyprVPN](#) is run by the Swiss-based global consortium Golden Frog, with 70-plus server locations worldwide. Compatible with Windows, Mac, Android and Apple, it can be connected to up to three devices at once, with up to 256-bit OpenVPN encryption. While VyprVPN *does* keep connection logs, it does not keep usage logs. VyprVPN owns its own networks and data centers in Switzerland.

It also uses its own protocol called “chameleon,” which can completely hide the fact that you're using a VPN — very useful in environments where it can mark you as suspicious. It also allows you to change your IP address and appear local when traveling to countries that impose internet censorship or in schools and workplaces that impart restrictions. That will enable you to bypass blocked websites and content and maintain access to the unrestricted internet.

- [Tor Browser](#) allows you to use the web entirely anonymously, has its own browser interface and is similar to a virtual private network but has the advantage of being instantly available once TOR is installed — and it's free. Tor is also open-source and operated through distributed computers rather than a central server. So, it *can't* be “hacked” or invaded.

Tor has become much easier to use and even more secure since the Snowden and WikiLeaks revelations emerged, but it remains your more complex technology than a simple VPN service.

Using a private VPN reduces the amount of information you knowingly or unknowingly provide when you surf the web.

But even without one, there are things you can do. Start using only Google Chrome or Firefox — never Microsoft Internet Explorer (IE). Because, unlike IE, those browsers are easily customizable.

Chrome and Firefox allow you to customize for privacy. For example, on your personal Google Chrome installation, you could use the following free “extensions,” which can be found on Chrome's web store:

- Adblock prevents most tracking cookies and blocks banners, pop-ups, malware and more.
- Collusion shows, in real time, what information websites silently send and receive to and from other websites that you never directly visit, so you can stop it.
- HTTPS Everywhere, which encrypts my web traffic on most sites. This free and open-source browser extension automatically makes websites use a more secure HTTPS connection instead of HTTP.
- IBA Opt-Out prevents Google and other sites from tracking your browsing habits for advertising purposes.

Combined, these little tweaks could make you nearly impossible to track. But just to be safe, you'll also want to disable almost all the tracking features on Google and ensure that you log out of Facebook and Google (including Gmail and YouTube) when browsing. Because if you're logged in, those companies will be able to track most sites you visit for marketing purposes.

Phase 4: Cloud Storage

When dealing with a large amount of private data, it needs to be stored somewhere with iron-clad security.

To do this, you'll need to ensure that whatever cloud storage platform you use can be encrypted.

Per TechTarget: "Encryption is the method by which information is converted into secret code that hides the information's true meaning."

It explains:

When an encrypted message is intercepted by an unauthorized entity, the intruder has to guess which cipher the sender used to encrypt the message, as well as what keys were used as variables. The time and difficulty of guessing this information is what makes encryption such a valuable security tool.

So encryption is the No. 1 feature you'll want to look for when selecting a secure cloud company to store your private data.

To help you make the best decision for you, I've included two top options below:

- **SpiderOak.** [SpiderOak](#) is a U.S.-based cloud storage company that has offered client-side encryption, which allows you to encrypt data locally since 2007. The encryption keys and password through which the keys are generated are stored on your device to ensure that no one can view your data.

SpiderOak also has an open-source software, Crypton, that provides developers with a simple way to build secure applications. Crypton's software essentially allows applications to encrypt information within a web browser before sending it to a remote server. SpiderOak supports Windows, OS X and Linux and has mobile apps for iOS and Android.

- **Tresorit.** [Tresorit](#) is a Swiss-based company founded in 2011 by Hungarian programmers Istvan Lam, Szilveszter Szebeni and Gyorgy Szilagyi. However, Tresorit officially launched its secure cloud storage service after emerging from its beta in April 2015.

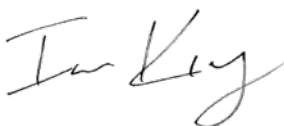
Tresorit has what the company calls "one of the strongest encryption algorithms on the market," making it possible to store and share data without the company's servers accessing the content. The company also has its DRM feature that provides more control for businesses by extending security to documents once they have been shared.

It allows you to modify or remove access to your encrypted content anytime — even if someone has already synced it to their computer. It also gives you access to more granular permissions, limiting copying, printing, screenshotting and more. Tresorit supports all major platforms, including Windows, Mac, Android and iOS.

We've covered everything from internet tracking and web browser security to cloud storage and social media precautions — all the necessary tools to spy-proof your digital footprint.

And with these tools, you can take back control of your private information, identity and most importantly, financial security.

Regards,



Ian King
Editor, *Strategic Fortunes*



Banyan Hill

P.O. Box 8378

Delray Beach, FL 33482 USA

USA Toll Free Tel.: (866) 584-4096

Email: <http://banyanhill.com/contact-us>

Website: www.banyanhill.com

LEGAL NOTICE: This work is based on what we've learned as financial journalists. It may contain errors and you should not base investment decisions solely on what you read here. It's your money and your responsibility. Nothing herein should be considered personalized investment advice. Although our employees may answer general customer service questions, they are not licensed to address your particular investment situation. Our track record is based on hypothetical results and may not reflect the same results as actual trades. Likewise, past performance is no guarantee of future returns. Certain investments carry large potential rewards but also large potential risk. Don't trade in these markets with money you can't afford to lose. Banyan Hill Publishing permits editors of a publication to recommend a security to subscribers that they own themselves. However, in no circumstance may an editor sell a security before our subscribers have a fair opportunity to exit. Any exit after a buy recommendation is made and prior to issuing a sell notification is forbidden. The length of time an editor must wait after subscribers have been advised to exit a play depends on the type of publication.

(c) 2023 Banyan Hill Publishing. All Rights Reserved. Protected by copyright laws of the United States and treaties. This report may only be used pursuant to the subscription agreement. Any reproduction, copying, or redistribution, (electronic or otherwise) in whole or in part, is strictly prohibited without the express written permission of Banyan Hill Publishing. P.O. Box 8378, Delray Beach, FL 33482 USA. (TEL.: 866-584-4096)