Artus GROUP
INVESTIGATIVE SERVICES

Take back your life

Start building your own wall of digital privacy

By **Rob Artus**, July 2023

Many of my recently divorced or separated clients routinely ask me the same questions:

1. How can I protect my digital privacy?
2. Have I been compromised electronically?
3. How can I be certain my former spouse or partner does not still have access to my devices, my location and my information?

Having helped many clients resolve these exact concerns, I've put together this instructional PDF to help you build your own wall of security – step-by-step, brick-by-brick.

What we're covering here:

Why a **burner phone** is your top priority

The importance of a **new Gmail account**

Why setting up **two-factor authentication** is so critical

Changing your **passwords** is a pain but is the next vital brick in your wall

How and why should you manage your **location** and **family sharing settings**?

Keeping your **PII** private

How to manage your **Apple ID**

Electronic sweeps, phone forensics, WiFi and **apps**

What else can you do?

Build your wall around you - BRICK BY BRICK

Clients going through a divorce or breakup can easily become overwhelmed. Attorneys, courts, investigators, accountants, parenting plans, fighting, mental anguish – it can leave them feeling exhausted, vulnerable and exposed.

As a result, digital security is sometimes the last thing on their minds or, they want to become more secure but **don't know where to start.** Often, clients are still using the same phones, accounts, passwords and settings as when they were married, and they don't know if their personal information, devices or accounts have been compromised. Especially if they are not technically savvy and didn't set up their accounts initially.

But there are many things you can do, and I like to think of the process as you building a wall of security around you, one brick at a time. You're not going to try and build the whole wall in one day, but each day you can add a brick and each week your wall will become higher and stronger. It takes patience, but if you can **make just one improvement each day**, your wall will grow.

Having helped many clients strengthen their digital security for many years, the following are some of the things I know you can easily do to help you take your life back. Make most,

or even some, of these changes and you will soon be on the road to freedom, safety and peace of mind.

As overwhelmed as you may feel right now, remind and comfort yourself that even the highest and most secure wall begins with the laying of a single brick.

You can do this. Let's get started – let's start building your wall:

Get a BURNER PHONE – today, before you do anything else

Many clients fear that their mobile phone(s) may have been compromised, or that their former partners may have access to their phone accounts, records and statements. If either of these are a possibility, go in person to one of the major phone stores and buy a prepaid mobile phone, and pay CASH only. Do not give a credit card, as it can be traced to you. And, when you update payment for future months, also only pay cash, physically in the store. Remember, no electronic trace helps keeps you anonymous.

When you go to these mobile stores, if they require your ID and real address information, then go to the next. Many of the major mobile carriers do NOT require any ID for prepaid phones purchased in-store, or your actual name or address – we have dozens of phones purchased by John Smith's and Sally Jones's from 123 Main Street, Bridgeport, CT and the like.

If you can't get a prepaid deal that includes an actual phone, simply buy a cheap phone online through Amazon or Walmart and then buy a prepaid SIM card in person at the mobile phone store (again with cash and anonymous ID). No one is going to trace the actual phone itself if you use a credit card – it's the actual number where you need the anonymity. It's remarkably simple to put the SIM card into your new phone and there's no activation process – the SIM card will just immediately work once it's in the phone. Most prepaid accounts will give high-usage phone and data plans, which is more than sufficient for your needs at this moment.

You **must** buy a new phone however: don't just buy a new SIM card and put it in your existing phone, as your existing phone may be compromised.

If you follow the above advice and pay cash without providing your ID and address, this new phone and the mobile account will be untraceable. You can then use this phone for your most private calls, such as to your attorney, PI, new beau or accountant. But as tempting as it might be, do NOT give out your new number or text with anyone that might be in contact with your former partner – and that includes your children and maybe even your parents.

Protect your new phone with a complex screen lock code (one you've never used before) or ideally with facial recognition, and DO NOT LET YOUR NEW PHONE OUTSIDE OF YOUR PHYSICAL POSESSION.

Create your new GMAIL account

Once you have your new, untraceable phone, the next step is to create a new Gmail email account. Gmail is preferable because there is no identifiable header information in emails sent or received via Gmail.

It's important that you set up your new Gmail account **on your new phone ONLY** at this time, and that you not set up or access your new Gmail account through your PC, laptop or other devices (which may be compromised). You can be certain that your new untraceable burner is not compromised, so create your new Gmail account from there.

For your new Gmail address, choose something simple and applicable, but do not include your years or dates of birth, children's names, personal identifying information, or frivolous names, as you will be using this email address for your private, official communication with attorneys, accountants and the like. When setting up this Gmail account, ensure you set up two-factor authentication (see below) and **do not set up the emails to forward** to your, or any other, email addresses.

Set up TWO-FACTOR Authentication on every account

Once you have your new, anonymous, untraceable phone and your new, uncompromised Gmail account, you can start adding two-factor authentication to all of your accounts. Setting up multi-factor authentication can be a pain, but it makes your accounts far more secure and is one of the most important things you can do – on all of your accounts.

Two-factor authentication adds additional layers of security to the standard password process. With two-factor, you will be prompted to enter one additional authentication method such as a code, which can be texted or called to your cell phone in what is known as a "short code" – I'm sure you've received them from many other accounts. It is often a five or six digit code.

You must set up two-factor authentication to send the short codes to your new burner phone and/or your new Gmail address (not your existing phone or existing email address, as they may be compromised, **which would defeat the whole purpose).**

Once two-factor authentication is enabled, any person attempting to access any of your accounts will need to know the short code, which has been sent only to your new, untraceable cell phone. Hence, they will not be able to access any of your accounts. Start with your email accounts, bank accounts, and social media accounts and then gradually go through all of your apps – even down to your TV subscriptions.

You can even enable multi-factor authentication for even greater security, where you will be prompted to enter more than one additional authentication method, such as facial identification or email, in addition to a text.

Setting up two-factor authentication is a critical component to your digital and personal security.

Don't try and update every account all at once, rather, try to make steady progress and add two-factor to maybe just one or a few accounts a day. Remember, build your wall one brick at a time and you'll soon be on your way to taking your life back.

Change your passwords, Change your passwords, Change Your Passwords!

Once you have set up two-factor authentication on your accounts from your new, untraceable phone and new, uncompromised Gmail account, **you MUST change your passwords** on all of your accounts, ensuring each has two-factor. Here are some obvious, and not so obvious tips:

- Even though you will be using your new burner phone for your most confidential communications, it's still imperative that you secure your existing devices. If you have an Apple iPhone, **change your Apple ID immediately** (see our section on this below to help you) and again, ensure you've enabled two-factor authentication.

- When creating new passwords, pay attention to **strong password** requirements and do not use any passwords you've ever used before, or your kids' names and dates of birth etc. Start fresh here, today.

- Make sure every new password for every account is **new and unique**, and don't use the same password – or variations of the same password – for multiple accounts.

- **Don't share** any of your passwords with anyone.

- Don't use common, easily guessable passwords. A **strong password** is at least eight characters in length and includes a mix of upper and lowercase letters, numbers, and special characters.

- Make sure passwords and password hints are stored securely – do not write them down on paper or in a book.

- Take this time to also **change the default passwords** for any devices in your house — if your home router, smart light bulbs, or security cameras are still using "password" or "1234" as the password, change them.

- Maybe not immediately, but in time, select a secure password storage app on your new untraceable phone only, one that automatically generates extremely complex passwords and then saves them securely in one place. I personally like and use **1Password** and some prefer **LastPass,** or others. All of these apps can generate passwords, monitor accounts for

security breaches, suggest changing weak passwords, and sync your passwords between your computer and phone. Password managers may seem intimidating to set up, but once you've installed one you just need to browse the Internet as usual. As you log into accounts, the password manager saves your passwords and suggests changing weak or duplicate passwords. Over the course of a couple of weeks, you end up with new passwords for most of your accounts.

- If you use the **1Password** app or similar, of course, only use any password app on your new untraceable phone, and make sure your "master" password for 1Password is something that no one else could ever guess, but one which you could always remember. You will be prompted by the app to enter your master password every two weeks, so, rather than a jumble of letters and numbers that you would have to write down and carry with you to re-enter (which defeats the purpose), select a memorable phrase. This phrase should be punctuated by unique characters and numbers to fulfill the password requirements. For example, select maybe a line from a song and the date the titanic sank, or a phrase your dad once said to you and the score you got on that fateful physics test – whatever you choose, select a phrase **you could never forget**, even under stress, but which **no-one could ever guess,** however many times or variations they tried**.** Here are some very basic examples of phrase passwords:

    - So-goodbye-yellow-brick-road-1912!
    - **You*are*my*genius*Jackie*48**

- However, **do not use this unique phrase for any other account.** Think of your 1Password master password as the key to the front door of your house – once someone gets in, they have access to everything. Don't write it down unless you can keep it in a locked safe, or give it to a parent for safekeeping etc.

How to Manage Your APPLE ID Account

An Apple ID is the main account that is required to use any of Apple's services, including the App Store, Apple Music, the iTunes Store, as well as iCloud. The Apple ID is essentially your identity on your iOS and Mac devices, and lets the device know who is currently using the device. If you use an iCloud account, you already have an Apple ID.

How to check Apple ID on iPhone or iPad

To check which Apple ID is currently logged in on an iPhone or iPad is very easy:

1. Launch the Settings app.
2. Tap the **Apple ID** Name & Photo at the top of the screen.

Here you can find any information about the Apple ID currently signed in on the iOS or Mac device. Using the options listed on this screen, you can also change Apple ID or Sign Out of an Apple ID on iPhone or iPad.

How to change Apple ID on iPhone or iPad

Signing out of your Apple ID and signing in with a new one can be done in the two basic set of steps listed below, and should take no more than 3-5 minutes:

Sign out of Apple ID on iPhone or iPad

1. Launch the Settings app on your iPhone or iPad
2. Tap the Apple ID Name & Photo at the top of the screen.
3. Scroll down a bit and then tap the Sign Out link.
4. If you use the same account for iCloud and the iTunes Store, you'll be asked to enter your Apple ID password. If you use two different accounts, you'll be given three options:
5. Sign Out of iCloud and Store
6. Sign Out of iCloud
7. Sign Out of Store
8. Select which data from iCloud you want to keep on the device and which data you want to delete using the toggle switches.
9. Tap Sign Out again to remove the Apple ID from your iPhone or iPad.

Sign In with a Different Apple ID on iPhone or iPad

Now that you have managed to remove the Apple ID that was previously being used on an iPhone or iPad, here's how you can Sign In with a different Apple ID on the iOS device.

1. Launch the **Settings** app on your iPhone or iPad.
2. Tap the **Sign in to your iPhone/Sign in to your iPad** link at the top of the screen. If you see a Name or Photo here, follow the steps outlined in **Part I** above.
3. Enter the **email address** or **phone number** associated with the different Apple ID you want to Sign In with.
4. Enter the password.
5. If you already have some data on your device, such as Contacts, Calendars, Bookmarks, etc., you will be asked if you want to Merge that data with this new Apple ID you are Signing In with. Tap **Merge** if you want to merge data, otherwise, tap **Don't Merge**.

How to change Apple ID on iPhone or iPad

Not many people are aware of this, but it is possible to sign in and use multiple Apple IDs on an iPhone or iPad. You can log in and set up multiple Apple IDs on an iOS device from the Settings app, and use them for different purposes like contacts, email, notes, bookmarks, etc.

For example, you may have a personal Apple ID that you use with the App Store and iCloud, but a different Apple ID for work purposes where you store your business or work contacts. You can set up two or more Apple IDs on an iPhone and iPad. Here's how:

1. Launch the **Settings** app on your iPhone or iPad.
2. Scroll down a bit and tap on **Passwords & Accounts**.
3. Tap **Mail** (or Contacts, Notes, Calendar) and tap **Add Account**.
4. Tap **iCloud**.
5. Enter the Apple ID email and password.
6. Select which services you want to enable for this Apple ID.

WiFi

Your digital security can be compromised using WiFi, so here are some tips to add some more bricks in your wall of security:

- **Change your WiFi password** using extra strong passwords.
- **Do not share** your WiFi password with guests – they'll just have to use 5G for the time-being until you feel more secure with your digital privacy.
- Do not trust public WiFi security without using a **Virtual Private Network** (VPN).
- Avoid connecting to **unsecured public WiFi** networks.
- Don't check your bank account balance or pay bills using public WiFi networks, in airports or coffee bars especially. **Not all public networks are secure**.

Personal Identifiable Information

It's very important that you protect your **Personal Identifiable Information** (PII), always. PII includes information such as your name, address, phone numbers, date of birth, Social Security Number, IP address, location details, or any other physical or digital identity data. So:

- Be extremely cautious about the information you include online.
- Don't reveal everything about yourself on social media – no one needs to know your date of birth, where you grew up, your mother's maiden name, your entire history and other PII Hackers use this information to their advantage and posting it will significantly increase your risk of a security breach.
- Do not send your PII or sensitive information over text message or email.

- Review your privacy settings across all of your social media accounts, particularly Facebook, and set them to private as much as you can. No one needs to know who all your friends are, or what you post, except your friends.

- There is almost never a reason to share your Social Security number with anyone online and if you are prompted to share it, take the time to research and be absolutely certain the request comes from a legitimate source. Remember, the IRS is NOT going to email you to confirm your Social Security number!

Apps

Every obscure app you install on your phone and every browser extension or piece of software you download from an untrustworthy website represents another potential privacy breach and security hole. Countless mobile apps track your location everywhere you go and harvest your data without asking consent, even in children's apps.

Stop downloading unknown software, and only download programs and browser extensions directly from their makers and official app stores. You don't need half the apps on your phone, and removing apps you don't need can also make your phone work faster.

Should you have your existing phones and devices analyzed?

Yes.

And No.

The issue with forensic phone and computer analysis is that it is often expensive. So, if you want to know for court or other relevant reasons, then yes, have them analyzed to see if they've been compromised – we've seen some serious breaches by ex-spouses and partners, and the findings have helped paint the picture in court. I do understand if clients want and need to have their devices analyzed – especially in situations where they have to continue to use their existing phone numbers and email address for work, for example.

However it is often much cheaper to buy new phones, laptops and devices than it is to have them analyzed and, if you follow my advice from the top of this article, building your new security wall is all about getting new devices, new phone numbers, new email accounts – all with new passwords and two-factor authentication, with location and sharing settings turned off.

I would say that yes, if money isn't an issue and/or you need to maintain usage of existing phone numbers and email accounts for work, then by all means forensic analysis will make sense and bring you peace of mind. Otherwise, just replace them and start your life anew.

How can you know if there are cameras, listening devices or tracking devices in your home and car?

You can't.

Unless you have your home and vehicles electronically swept.

Electronic sweeps are known by several names, including "debugging" and "TSCM" (technical surveillance counter measures), but for the purposes of this article, I'll call them "sweeps". Our team will come to your home and, depending on square footage and number of rooms, will spend the day sweeping everything in search of listening devices, cameras or any areas in which your property might have been compromised.

Our sweeps include analysis of radio signals, a variety of electronic tests, and a physical security review of all designated areas. Radio signal analysis includes inspection of WiFi, Bluetooth, and cellular frequencies looking for any suspicious signals or other anomalies. Other tests include thermal imaging, non-linear junction detection (for hidden electronics), as well as a visual and physical search.

At Artus Group, we have a wonderful team who are recognized as the best in the Northeast, and their work is government grade. Simply put, they can bring you immense peace of mind: if they say there's nothing there, then there's nothing there. Having said that, they've found some outrageous devices and invasions of privacy.

Electronic sweeps conducted at this level are not inexpensive, but they sure do provide the peace of mind you need to move forward with your life.

Can I search my own car for GPS trackers?

We can certainly add cars to any sweep, with the primary focus being on listening and tracking devices. Again, it is not inexpensive, due to the technical equipment and skill of the technicians, but I always recommend it. Some devices are so cleverly hidden that physical inspection alone can't find them.

Having said that, there are certain basic steps you can take to **check for yourself** to see if there is a **tracking device** on your car. It's not a comprehensive search of course, but it's something you can do and, after all, many ex-spouses and ex-partners are not all that clever or thorough.

Here are some things you can do:

1. As you probably know, even the most basic GPS tracking devices are now inexpensive and have surprising distance and battery range. Physically inspect the inside and outside of your car. Look for any unusual looking packages, devices or boxes. This includes under the seats, in the spare-wheel area in the rear, deep in the center console, in the flap behind the front seats etc. If you find something that is unfamiliar or doesn't look or feel like it belongs, take a photo and call me.

2. More sophisticated GPS tracking devices can be placed inside the wheel wells of the car (the recess area inside your fenders that house the wheels) or under the car. **Ensuring the vehicle engine is off and the parking brake is on**, you can get a flashlight and look around each wheel well – the wheel wells and your tires will be dirty, so wear gloves. The wheel wells are often the best place to place a GPS device because the wheel well is usually metal, and persons placing GPS devices often do not have access to the inside of the car. So, they lock the GPS tracker inside a metal box – such as an Otter Box - on which heavy duty magnets have been placed. All they have to do is then kneel down next to the wheel, clamp the magnetic Otter Box inside your wheel arch, and walk away – it takes less than five seconds. Go ahead and search your wheel wells and, **without putting any part of your body under the car**, scan your flashlight on the undercarriage and look for an Otter Box or similar. A real amateur might secure their tracker with rudimentary tape wrapped around and around a suitable receptacle, so look for anything taped, as well as the magnetic box type of containers. Again, if you see anything suspicious, take photos and call me.

Although you can conduct a few rudimentary searches yourself, electronic sweeps are like doing your own surgery: you have no idea what you are doing and you don't have the equipment or expertise. So call me and we'll get our experts to bring you some peace of mind.

LOCATION SETTINGS

There is a lot to know and do regarding your location settings, but it's imperative that you not share your location through your phone or other devices. Here's what you need to know:

How to turn Location Services on or off for specific apps

1. Go to Settings > Privacy & Security > Location Services.
2. Ensure Location Services is on.
3. Scroll down to find the app.
4. Tap the app and select an option:
    a. Never: Prevents access to Location Services information.
    b. Ask Next Time Or When I Share: This allows you to choose Always While Using App, Allow Once, or Don't Allow.
    c. While Using the App: Allows access to Location Services only when the app or one of its features is visible on screen. If an app is set to While Using the App, you might see your status bar turn blue with a message that an app is actively using your location.

d. Always: Allows access to your location even when the app is in the background.

How do I know if someone can see your location on iPhone?

To see who can track your location, open up the Find My app and tap on the "People" tab. People who have shared their location with you and people you have shared your location with will show up in this list. A person who is able to see your location will be denoted with "Can see your location."

Determine Who Is Allowed To Track Your Location with Find My

If you have granted location access to your friends or family, they can track your whereabouts through the **Find My** app. To determine who can track your location, open the Find My app on your phone and tap on the "People" tab.

People who have shared their location with you and those you have shared your location with will appear on this list. Any individual who is able to see your location will be denoted as "Can see your location."

Tap on any person's name in the list and you can get to settings that will allow you stop sharing on an individual basis. Just tap on "Stop Sharing My Location" to block that person from tracking where you are.

Sometimes people who can see your location do not have the "Can see your location" designation, so be thorough and check each name in the list.

You can also get to these settings by opening up the Settings app, going to the Privacy section, selecting Location Services, and then choosing "Share My Location." This shows you a list of family and friends who are able to see your location.

Tap on any of the listed names to get to an option where you can toggle off location sharing.

Prevent People from Tracking You with Find My

There are two ways to make sure no one is following your location through the Find My app: either through the Find My app itself or through the Settings app on the iPhone.

To use the Find My app:

1. Open up Find My.
2. Tap on the "Me" tab.
3. Toggle off "Share My Location."

To turn off Location Sharing in the Settings app:

1. Open the Settings app.
2. Tap on Privacy.
3. Tap on Location Services.

4. Tap on Share My Location.
5. Toggle off "Share My Location."

Protect Location Information Even While Using Family Sharing

With Family Sharing you and up to five other family members can share access and content within various Apple services and app subscriptions. If you have Family Sharing enabled, you will automatically appear in the People tab for each person you are sharing with, but utilizing the steps above to disable location sharing will prevent your family members from tracking where you are.

Even with Family Sharing turned on, all parties involved must agree to share location data, and you should double check your Family Sharing settings to make sure location is disabled.

1. Open the Settings app.
2. Tap on Family Sharing.
3. Under "Shared With Your Family," tap on "Location Sharing."
4. Make sure "Share My Location" is toggled off, or tap on an individual family member's name to turn off location sharing on a per person basis.

Identify Which Apps Can See Your Location

Apps can request access to your location, and if you're using social networking apps like Snapchat, Instagram, or Facebook, it is certainly possible that your actions on those sites could have location information attached.

To identify which apps have access to your location, follow these steps:

1. Open the Settings app.
2. Scroll down to Privacy.
3. Tap on Location Services. Scroll down to see the location permissions for each of your installed apps.
4. To change location permissions, tap on any app name in the list and select "Never" if you want to make sure the app does not have any access to your specific location through iOS.
5. There are other location options such as "Always," "While Using the App," and "Ask Next Time," but these are not ideal if you're goal is to prevent the app from seeing your location entirely.
6. Using the App allows your location to be shared when you're actively using the app, but cuts it off when you're not using it. Ask Next Time will prompt the app to ask for your location the next time you use it, and Always will leave location access on permanently.
7. With some apps, you'll also see an option for "Precise Location". If you turn this off, an app can determine your general location, but it is an approximate location rather than your specific location.
8. Be aware that even with location services turned off, apps like Facebook can track your approximate location through IP addresses and other similar means, which is something

to consider. Most of this tracking is done behind the scenes and is not accessible to individuals.

Turn Off Your Location Exclusively (Safest Option)

If you want to be absolutely certain that no person or app can track your location through the GPS and Bluetooth systems built into your iPhone, it's best to turn Location Services off entirely.

WHAT ELSE CAN YOU DO?

We've covered a lot in this PDF, but here are some extra layers of security to keep your accounts and data safe:

- Back up important personal information on external hard drives or a cloud account – I recommend and use **Carbonite**.

- Don't review private and financial information on **public computers**. If you need to use a computer at a hotel, library or other public space, make sure you log off all accounts and clear your browsing history.

- Contact Experian and TransUnion to put a **lock on your credit accounts** so no one can open new credit cards or get loans using your credit history and identity. This will also ensure your ex-partner cannot run your credit report to see what new accounts you have opened, or what balances you carry.

- **Pay with Your Smartphone:** The system of credit card use is outdated and actually not very secure at all. Instead of using your physical credit card, use Apple Pay or an Android equivalent everywhere you can. There are many choices when it comes to apps and setting up your smartphone as a payment device is typically a simple process, sometimes as simple snapping a picture of the credit card that you'll use to back your app-based payments. If you see any **suspicious charges** on your debit or credit card, utilize mobile banking card controls to turn off your card, and contact your bank immediately.

- Make sure you only enter your financial information on **legitimate apps and websites**. Cybercriminals will sometimes create copycat websites and apps to trick people into entering their personal information on an unsecured site. Check the URL of the website you're on before entering your account information.

- **Update apps frequently** because they often contain important security upgrades. Outdated apps are more hackable and more susceptible to data breaches.

- **Phishing scams use fraudulent emails** and websites to trick users into disclosing private account or login information. Here are a few vital steps you can take:

1. Do not click on links or open any attachments or pop-up screens from sources you are not familiar with.
2. Don't open email from people you don't know.
3. Know which links are safe and which are not – hover over a link to discover where it directs to.
4. Be suspicious of the emails sent to you in general – look and see where it came from and if there are grammatical errors.
5. Malicious links can come from friends who have been infected too. So, be extra careful. If it doesn't feel right, don't open it and give them a call.

- **Hackers can use social media** profiles to determine your passwords and answer those security questions in the password reset tools. Lockdown your privacy settings and avoid posting things like birthdays, addresses, mother's maiden name, etc. Be wary of requests to connect with people you do not know. The app generates a one-use authentication code, good for the current transaction only. Even if someone filched that code, it wouldn't do them any good. A common scam starts with a private message and ends with hackers taking over your account and using it to continue the scam. If you get an odd or unexpected private message from a friend, ask about it using email or some other type of communication. Your friend may have been scammed.

- You can drastically **reduce the amount of data going to Facebook** by disabling the sharing platform entirely. This will help ensure your personal data isn't leaked. Google also knows a lot about you, maybe even more about you than Facebook, so take steps **to manage your Google privacy**, too.

- Think twice before revealing too much in a post, since your friends might share it with others. With care, you can retain your privacy without losing the entertainment and connections of social media.

YOU'VE GOT THIS

All of the above information may seem like a lot to take in and of course, no one can do everything in one day. But if you can take it one day and one fix at a time, you can build your own wall of security around you, step by step, **brick by brick.**

Good luck, and call or email me if you have any questions.

Rob Artus
Artus Group, Inc.
rob@artusgroup.com
860-463-9118

About Rob Artus

In 2004, I saw the need for an innovative private detective firm, one that provided a whole new level of professionalism and quality. I formed Artus Group, which I am very proud to say is now one of the more highly respected boutique firms in the country. We continue to grow and attract new clients through perseverance, expertise and common sense…with no fluff.

I've managed major investigations worldwide and have personally investigated thousands of corporate fraud investigations, due diligence cases, background checks, asset searches and family investigations. I'd like to think of myself as a specialist in family litigation investigations, and I've testified in court on numerous occasions.

I've developed an extensive portfolio of worldwide resources and am an active member of the Council of International Investigators and the international intelligence network, Intellenet. I served as Chairman and co-founder of the Connecticut Private Investigators Association; was a former board member of the Connecticut Association of Licensed Private Investigators; and enjoyed a long and rewarding membership of the Life Solutions Center of Darien.

I am pleased to share with you everything in this PDF and will be more than happy to get on the phone and help you even further if you have the need.

Until then, good luck, build your wall brick by brick, day by day, and take back your life. You've got this!

Rob Artus
Artus Group, Inc.
rob@artusgroup.com
860-463-9118

Visit our website

See what our clients say about us