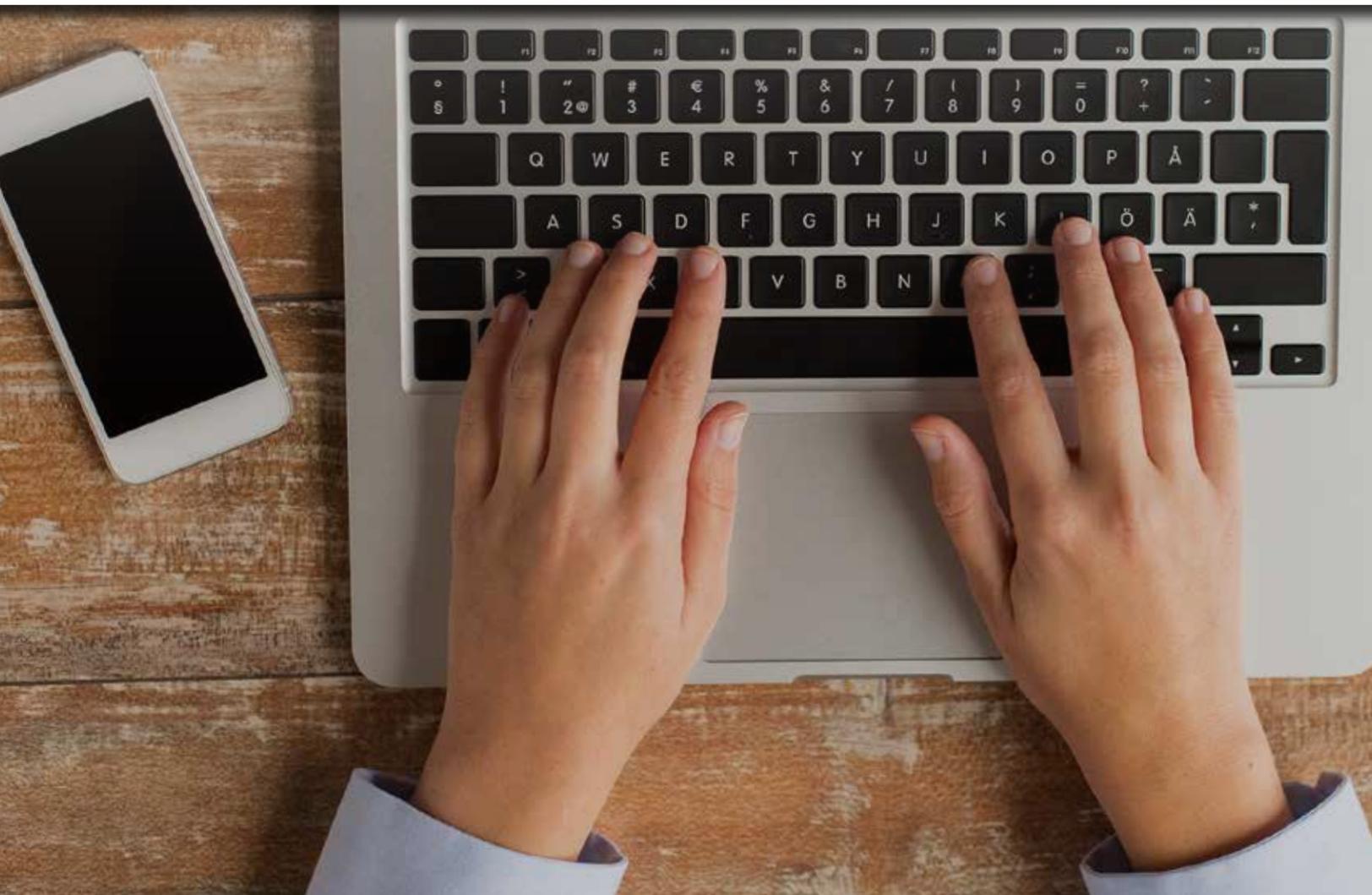




7 Free Ironclad Tools for
**Protecting Your
Money and Privacy in
Today's Digital Age**





7 FREE Ironclad Tools for Protecting Your Money AND Privacy in Today's Digital Age

By Ted Bauman, Editor, *The Bauman Letter*

THE thieves' plan was as faultless as it was daring.

The object was in a safe on the third floor of a Venetian townhome on the Calle Larga Mazzini. Posing as painters, they gained entry to the apartment below and primed the ceiling with tiny amounts of plastic explosives. They did the same to the ceiling of the boathouse under the building.

At the flick of a switch, the explosives detonated, simultaneously breaching the floors and dropping the safe into a vessel waiting in the boathouse. The pilot gunned the engine, and they were gone.

The outraged owners of the safe could do nothing. They were only prepared for conventional threats.

But if the material inside the safe was useless ... the thieves would have nothing.

In the film *The Italian Job*, the industrious gang of burglars gets what's in the safe, albeit with many twists in the tale.

But imagine a scenario in which the safe's purloined contents remained useless to them, even after they cut the safe open and held the item in their hands. They could see it and touch it, and knew what it was worth. But they couldn't do anything with it. The rightful owners of the property had taken steps to render it useless to anyone but them.

The movie safe held gold. But there's another form of wealth that's just as important, and which can be protected in a way that leaves even the cleverest thief high and dry: personal information.

Consider who's after that information. We know about the National Security Agency, the FBI and other government agencies that routinely abuse our privacy rights. For example, no one has Fourth Amendment privacy rights when crossing the U.S. border. Border agents can copy all the files off your computer or phone. This is true around the world.

Private companies take your details and store them on servers which can be hacked. Websites are tracking your every move on the internet and pass that information on, for profit, to lawyers, business competitors, estranged family member and blackmailers. Even ATMs can be compromised by hackers looking to steal information from the ubiquitous magnetic stripes on the backs of all but the most advanced bank cards.

You need to secure your information. It's just as important as any physical asset. In some cases, it's even more so.

That's why I've compiled this report for you, which details seven free ironclad tools for protecting your money and privacy in today's digital age...

- **Tool No. 1: Windows Encryption**
- **Tool No. 2: Mac Encryption**
- **Tool No. 3: Apple Pay**
- **Tool No. 4: Google Wallet**
- **Tool No. 5: PayPal**
- **Tool No. 6: Other Apps**
- **Tool No. 7: i-Account**

But in order to understand and use these tools properly, I want to take a brief moment to talk about two important concepts: file encryption and how to create a strong password.

Encryption Security in the Digital Age

I know it sounds strange, but in order to make your personal information truly secure, you first need to turn it into digital form.

All of us have important paper documents. I routinely scan all of mine — passports, birth certificates, receipts, warranties and so on — to Adobe Acrobat (PDF) files and store them on my home computer. Simple enough. But then I back up all the files on my home computer to a special hard drive contained in a small fire- and waterproof safe that has a network connection built into its side.

Every day my computer automatically backs up my data to that drive, which is bolted to the foundation of my house and accessible via a hidden door in the basement floor. Even if a gas leak blew the place up or a tornado roared through, I'd still have digital copies of my records.

And because it's so small and hidden away, that safe would be overlooked by any thief. But even if a thief found it and pried it loose, I'd still be fine.

That's because I also store my important records in the "cloud," using an automatic online backup system on secure servers in Switzerland. It costs me very little ... about \$5 a month. I can access those servers from anywhere in the world.

Digital records can't replace all physical documents, of course. But having digital copies of the key ones makes it infinitely easier to replace them.

So consider what personal information you have in your home that's important to you, where it is and what threats it might face.

The fact is that any personal information in physical form — photos, birth certificates, marriage documents, wills, business records — is vulnerable to theft and destruction. Few people have big fire- and waterproof filing cabinets and safes.

However, once you've created digital copies, you're now vulnerable to digital theft...

Unless you take my first step and encrypt it.

But what about hackers? And the NSA? And the FBI? Am I just making their job easier by digitizing everything?

Not at all. That's because everything on my computer and in the cloud is encrypted.

NSA whistleblower Edward Snowden — who knows a thing or two about encryption — maintains, "Encryption works. Properly implemented strong crypto systems are one of the few things that you can rely

on.” And if the directors of the FBI and the NSA don’t like encryption — they hate it — it must be worth it.

Encryption is used at many different stages in the handling of digital information. The two most important are when information is in storage and in transit.

In this report, the focus of Step 1 will be on the encryption of stored digital information, such as the files on your hard drive.

The technique I use to protect my digital assets at home is called full-disk encryption. Full-disk encryption is the easiest way to protect your data in case your computer is stolen or breached. It works on both laptops and home PCs.

How Encryption Works for You

The goal of disk encryption is to prevent someone who gains access to your computer — such as a lost or stolen laptop — from reading the files stored on it.

Encryption works by scrambling digital information into seemingly random sequences of letters, digits and symbols. It can only be unscrambled with a special “key.” It takes minimal effort to encrypt your entire disk at once, a task that can be completed in under an hour.

Here’s how full-disk encryption works.

When you turn your encrypted computer on, before your operating system — such as Windows or Apple Mac — can boot up, you must first “unlock” your disk by typing in a password or (even better) a passphrase. This in turn unlocks a special encryption key on your disk, which then unlocks everything on the disk for as long as the computer remains on.

Once your computer is on and you’ve entered your passphrase, your disk is completely transparent to you and to the applications on your computer. Files open and close as they normally would, and programs work just as they would on an unencrypted machine. You won’t notice any performance impact.

But without disk encryption, if someone gets physical access to your computer — like the several laptops I’ve had stolen in my travels over the years — they can easily see the content on all your files.

What if you have a strong Windows password? It won’t matter at all. That’s because an attacker can simply boot your computer to another operating system from a USB stick, bypassing your password, to look at your files. Or they can remove your hard disk and put it in a different computer.

But with strong disk encryption, they won’t be able to read a thing on your computer’s drives — ever.

Note that disk encryption is only useful against attackers who have physical access to your computer. It’s still possible for your computer to be hacked and for individual files to be stolen when you’ve unlocked it and connected it to the internet. Disk encryption also doesn’t protect your activity on the internet.

For now, though, let’s focus on protecting your computer from unauthorized physical access.

Open-Source Encryption Is Your First Choice

As a rule, I prefer open-source software for security purposes. Open-source software is free and can be opened up and analyzed by anyone. That way any bugs or malicious privacy-defeating “backdoors” are impossible to hide.

My preference for open-source software includes encryption. If you want the security of using open-source software to encrypt your computers, I recommend DiskCryptor. It’s 256-bit encryption, managed by the

Electronic Frontier Foundation, one of the best outfits around dedicated to digital security. It's easy to set up and use and can be found here, along with step-by-step instructions: <https://ssd.eff.org/en/module/how-encrypt-your-windows-device>.

But if that's more than you want to bite off, here's another solution that's worth your time: Use the encryption tools built into Microsoft Windows or Apple OS X. Even though they aren't open-source, it's unlikely that the U.S. government knows how to hack them via hidden "backdoors." I personally don't believe that they can — after all, the British government failed to do so when they detained the partner of crusading reporter Glenn Greenwald at Heathrow Airport in 2013. And once you're comfortable with encryption using these tools, you can always shift to open-source software later.

The Trick to Creating the Right Password

Before I explain how to encrypt your computer's disk(s), let's look at the critical role of passwords or passphrases. Passwords are assessed in terms of "entropy." Entropy is measured in bits, and determines how many guesses it would take to crack the password.

For instance, a single password in 32-bit encryption would take 4,267,967,296 guesses to crack. It would take approximately a month and a half for a supercomputer to try all those guesses.

By contrast, a seven-word 128-bit passphrase like "waltzed assemble maverick tonsil subsumes gunner submarine" would require 165,874,258,366,850,931,470,183,446,872,064 guesses. At 1 trillion guesses per second, it would take 27 million years for supercomputers to crack this. That's why passphrases are the preferred approach to true digital security these days — not individual passwords.

There's a technique to generate totally random passphrases using dice and a word list. You roll a six-sided die five times, and write down the numbers that come up. If you roll the number two, then four, then four again, then six, then three, then look up 24463 in the Diceware word list (<http://world.std.com/~reinhold/dicewarewordlist.pdf>), you'll find the word "epic." That would be the first word in your passphrase. Repeat until you have a seven-word passphrase ... one that the NSA couldn't break in 27 million years.

Of course, with strong disk encryption you must be extremely careful. If you forget your passphrase, you'll be locked out of your own computer, losing your data forever. Nobody can help you. That's the point of disk encryption, after all. For that reason, memorization and/or secure storage of your passphrase is crucial.

My critical passwords, for example, are stored in two separate ways. The master encryption password is printed out, laminated to protect from moisture and stored in that little safe I mentioned. (If I had a safe-deposit box, I could also keep it there, but it would be vulnerable to court orders served on my bank.) I also keep an encrypted Excel file with a copy of my master password along with other important passwords and digital keys on the hard disk stored in my hidden safe, as well as on my encrypted cloud server. And I've given a copy of the master password to that encrypted file to someone I trust.



Tool No. 1: Encrypting Your Disk in Windows

Certain versions of Microsoft Windows 10 (as well as the Ultimate, Enterprise and Pro versions of Windows Vista, 7, 8 and 8.1) include BitLocker, Microsoft's disk encryption technology. It's not on the Home version, which often comes preinstalled on Windows laptops. BitLocker uses 128-bit encryption, which is incredibly powerful.

To see if BitLocker is supported on your version of Windows, open up

Windows Explorer, right-click on the C: drive and see if you have a “Turn on BitLocker” option. If BitLocker isn’t supported in your version of Windows, you can choose to upgrade to a supported version by buying a license. Open Control Panel, System, click “System” and then click “Get more features with a new edition of Windows.”

Now, you might think that this is too complicated to do yourself. You can ask a trusted friend or relative to help you if you feel uncomfortable with anything. You could also have a computer technician install it with a temporary password that you change later.

But believe me, it’s really not very difficult, and will take you only about 20 minutes plus about half an hour for the software to encrypt the disk.

BitLocker can be used with a Trusted Platform Module (TPM), a tamper-resistant chip built into new laptops and PCs that can store your disk encryption key. If your computer doesn’t have a TPM — something BitLocker will tell you as soon as you try to enable it — it’s possible to use BitLocker with a passphrase or USB stick instead.

I strongly recommend that you don’t use a TPM, even if there is one in your computer. If you do, your disk will be automatically unlocked when it’s turned on. Instead, you should set a special PIN to unlock your disk. This is a bit more complicated, but worth it for the extra security. Here’s how you do it.

Once you’ve turned on BitLocker, you’ll be prompted to make a backup of your recovery key, which can be used to unlock your disk in case you ever get locked out. Since it can unlock your disk, don’t save a copy of your recovery key to your Microsoft account (if you have one). If you do, Microsoft — or anyone with whom the company is compelled to share data, such as law enforcement or intelligence agencies, or anyone who hacks into their servers — will be able to unlock your encrypted disk. Instead, you should save your recovery key to a file on another drive, such as a USB stick, and/or print it out and store it securely as I’ve recommended.

Once you’ve done this, follow the rest of the instructions and reboot your computer. When it boots up again, your disk will begin encrypting. You can continue to work on your computer in the meanwhile.

Once your disk is encrypted, the next step will be to set a PIN. This requires tweaking some Windows settings, but it isn’t hard if you follow my instructions.

Click the Start button, and type “gpedit.msc” in the little box above it. Press enter to open the Local Group Policy Editor. In the pane to the left, navigate to Local Computer Policy > Computer Configuration > Administrative Templates > Windows Components > BitLocker Drive Encryption > Operating System Drives.

In the pane to the right, double-click on “Require additional authentication at startup.” Change it from “Not Configured” to “Enabled,” and click OK. You can then close the Local Group Policy Editor.

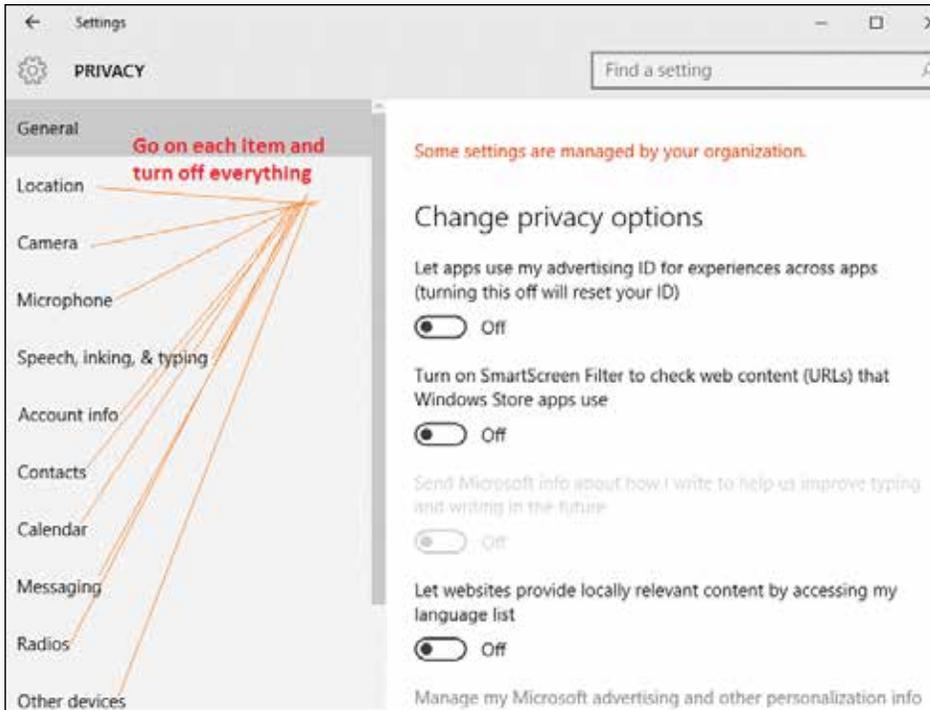
Now open Windows Explorer, right-click on drive C and click “Manage BitLocker.”

In the page that opens up, click “Change how drive is unlocked at startup.” Now you can choose between either entering a PIN when starting up, or inserting a USB flash drive. I recommend you use a PIN. If you are asked to open your computer while crossing a border, for example, you can choose not to type your PIN to unlock your drive. But if someone gets their hands on your USB flash drive, they can use that to boot your computer.

Your PIN must be between four and 20 numbers long. The longer you make it the more secure it is, but make sure the PIN is stored somewhere where you can retrieve it if needed, as I explained earlier.

After entering your PIN twice, click “Set PIN.”

Now reboot your computer. Before Windows starts this time, you should be prompted to type your PIN.



Windows 10 Anti-Spying Bonus: If you are running Microsoft’s Windows 10 operating system, it’s quite possible your computer is spying on you as you read these words. The reason is simple: Microsoft has adopted a business strategy made popular by Google, Facebook and other internet giants: They profit by gathering and selling users’ personal information.

Microsoft even discloses this in the fine print of their privacy statement for Windows users:

Microsoft collects information about you, your devices, applications and networks, and your use of those devices, applications and networks. Examples of data we collect include your name, email address, preferences and interests; browsing, search and file history; phone call and SMS data; device configuration and sensor data; and application usage. [...] We will access, disclose and preserve personal data, including your content (such as the content of your emails, other private communications or files in private folders), when we have a good faith belief that doing so is necessary to protect our customers or enforce the terms governing the use of the services.

Most, but not all, of the settings that Windows 10 uses to spy on you can be disabled by tweaking the security settings. Click on the Windows symbol in the lower left corner of your screen, select “Settings,” then click on “Privacy.” You can then disable most of the settings manually.

A much simpler solution that I have tested and scanned for spyware is [this anti-spy tool](#). I have researched and reviewed the company that makes it, a privacy-sensitive outfit in Germany, and I’ve used it on my own machine. It works and didn’t do any harm to my setup.

Tool No. 2: How to Encrypt Your Disk in Mac OS X



FileVault, Apple’s disk encryption technology for Macs, is simpler than BitLocker, but just as strong.

Open “System Preferences,” click on the Security & Privacy icon and switch to the FileVault tab. Click the lock icon in the bottom left so you can make changes, and click “Turn on FileVault.”

Next you will be asked if you want to store a copy of your disk encryption recovery key in your iCloud account. Don’t, for the same reasons I gave for BitLocker: If you do, Apple — or anyone with whom the company is compelled to share data, such as law enforcement or intelligence agencies, or anyone who hacks into their servers — will be able to unlock your encrypted disk.

Instead, choose “Create a recovery key and do not use my iCloud account” and click Continue. The next

window will show you your recovery key, which is 24 random letters and numbers. You can write this down and put it in a safe, and/or type it into an encrypted computer file.

Once you click Continue, you will be prompted to reboot your computer. After rebooting, FileVault will begin encrypting your hard disk. You can continue to work while it's doing this in the background.

Mac OS X user passwords double as passphrases to unlock your FileVault encrypted disk. For this reason, you should use a random passphrase like the ones I mentioned earlier.

Note: When You're Traveling...

Determined adversaries can beat disk encryption. But you can prevent that if you power off your computer completely when you finish working on it, or when you're outside your home with a laptop.

Here's why: Computers have temporary storage called RAM. When your computer is powered on, your software is constantly writing to and deleting from RAM. When you use disk encryption, as soon as you unlock your encrypted disk, the encryption key is stored in RAM until you power your computer off. This allows it to encrypt and decrypt files as you use your computer. Laptops have ports that have "direct memory access," or DMA, including FireWire, USB and others. If an attacker has access to your computer and your disk is unlocked — even when it's in sleep mode — someone can plug a malicious device into your computer and read its RAM, including your encryption key.

So remember to power off your computer when you're finished.

As you can see, with so much of our personal information in digital form — a form that has major advantages for long-term protection — learning encryption skills is the essential first step to becoming master of your own privacy.



Tool No. 3: Apple Pay

Apple-based payment apps are the most popular in every region of the globe. In most places, twice as many people use Apple-based apps as Android (which runs on most non-Apple smartphones). The only place where Android apps are close to Apple levels of usage is Asia. So it makes sense to start with Apple Pay.

Apple Pay works only on the iPhone 6 or later models, or the Apple Watch. You register your supported credit cards in the device's Passbook app. When you want to buy something from a retailer that supports Apple Pay, you point your device at the near field communication (NFC) payment terminal, and your payment information is delivered from your iPhone over a radio frequency connection. Then you do a fingerprint scan on your phone's Touch ID sensor to verify your identity. If everything is OK, your phone vibrates and tells you the transaction was approved. Apple Pay also works from within other apps, such as when you wish to purchase a plane ticket using an airline's app.

Apple Pay uses tokenization, to keep your transaction safe. Tokenization is essentially the process of substituting a sensitive data element with a nonsensitive equivalent (a token) that has no extrinsic or exploitable meaning or value. The token is stored on a special chip called a Secure Element. If the iPhone is lost or stolen, for instance, you can use "Find My iPhone" to suspend all payments from that device. There's no need to cancel your credit card, because the card information isn't stored on the device.

Apple doesn't get to know what you bought, how much you paid for it or any other personal details.

The guy behind the counter doesn't get to see your name or your credit card number — all of which are potential weak spots of the current system, under which cards are occasionally cloned and ripped off.

- **Where:** Apple Pay is rolling out rapidly in the U.S., U.K. and Europe. Apple is reportedly in talks with Australia and Canada to introduce the app. Two things are required to use Apple Pay: The merchant must accept it and your bank must authorize use of your card abroad. Currently, many major retailers, including Macy's, McDonald's and Walgreens, accept Apple Pay. Dozens of smaller merchants have already signed up, too. Apple Pay is also making rapid inroads in Asia, but with the popularity of Android smartphones there, it may take a little longer. In those regions, you can use local payment apps in the meantime.
- **Pros:** The safest system of all, with end-to-end tokenization and no storage of your card or personal details on Apple servers.
- **Cons:** You must upgrade to iPhone 6 or later, or an Apple Watch, to use it. Also, not all countries allow prepaid debit cards to be loaded into Apple Pay.
- **Whom it's for:** Essentially everyone who uses an Apple iPhone, especially in the U.S., U.K. or continental Europe.



Tool No. 4: Google Wallet

Like Apple Pay, Google Wallet involves tapping your phone on a POS terminal, entering your Wallet PIN and completing your transaction as usual. And like Apple Pay, Google Wallet uses tokenization — your real 16-digit card number is never exposed to merchants. But instead of securing the token in a chip on your phone, Google uses something called Host Card Emulation (HCE), which stores your token virtually in “the cloud.” This makes Google Wallet compatible with any NFC-equipped Android phone. The app also lets you store club cards and gift cards as well as credit and debit cards.

- **Where:** Widely available in the U.S. and expanding rapidly in the U.K. and Europe. Not yet available in most of the rest of the world.
- **Pros:** Extensive availability in the U.S., U.K. and Europe. Also, Google Wallet is potentially compatible with highly secure Android-based phones such as the Blackphone (although there are rumors that Blackphone is developing its own super-secure payment systems).
- **Cons:** In order to use Google Wallet in stores, you'll need an NFC-capable Android phone, which is only 25% of Android phones on the market right now. Major players such as Samsung are rapidly adopting NFC technology. If you aren't an Apple fan, you should choose one of their phones if you'd like to use Google Wallet in the future.

A second drawback is that the HCE technology Google has chosen requires that your phone be connected to your cell service to use, because the phone needs to retrieve its tokens from the cloud. That could be expensive if you're traveling abroad.

The biggest con, however, is that anything that operates in the cloud — instead of locally, on your phone, as with Apple Pay — is automatically more vulnerable to security attacks.

- **Whom it's for:** For security reasons, I would use Google Wallet only if you are resolutely opposed to Apple.



Tool No. 5: PayPal

Like Apple Pay and Google Wallet, PayPal transactions are tokenized and encrypted, and merchants never see their customers' complete identity, personal information or financial data. Plus, if your phone has a fingerprint scanner (like the Samsung Galaxy S7 and S7 Edge), you can use that to authorize transactions.

• **Where:** Restricted to U.S. merchants at the moment, particularly on the West Coast.

• **Pros:** Secure and widely accepted in the U.S. You also have the option to make purchases at credit card terminals using your phone number and a PIN code.

• **Cons:** Because it moved in early and missed some more recent technological innovations, PayPal has struggled to get merchants to sign on to its systems and is therefore likely to be eclipsed rapidly by Apple Pay. Like Google Wallet, you need cell service in order to use PayPal.

• **Whom it's for:** People who already have PayPal accounts and for whom adding another payment option is essentially costless. But it's not for overseas travelers.

My Overall Pick...

Apple Pay. It's significantly ahead of the competition, and given the iPhone's wide and deep penetration in the U.S., U.K. and Europe, it will inevitably set the standard for smartphone-based payment solutions in those areas, even for non-Apple services.



eWallet



SnapScan



Square



LevelUp

Tool No. 6: Other Apps

In today's world, the threats to your information are everywhere — even offline. For instance, ATMs, gas pumps and vending machines — nearly any stand-alone public device fitted to take credit cards — can be compromised with “card skimmers.”

A skimmer is basically a small, easily overlooked plastic device that thieves fit over the real machine's card slot. Each year, millions of people unwittingly insert their cards into card skimmers, which then copy the data off the card.

It was already a problem with the standard magnetic-stripe cards issued by most U.S. banks for the last 50 years. But experts say even the new chip-and-PIN cards are susceptible. Bad guys now often couple the skimmer device with a tiny hidden camera aimed at the machine's number pad, so

they can record your fingers tapping in your card's PIN code.

However, if you carefully absorb the advice I'm about to give, you can sidestep the fear and inconvenience that come with being financially compromised, particularly when you're abroad.

There are safe, simple solutions available to you that don't require complicated foreign banking arrangements and hassles. These solutions utilize the advances in transactional security that have largely bypassed Americans ... until now. You can transact abroad with confidence and security if you learn the secret to using them.

The first solution is using a payment app.

When I was visiting my second home of Cape Town, South Africa, one Christmas Eve, I came across an

ATM compromised by a card skimmer. So I downloaded a payment app on my Apple iPhone called SnapScan, developed by South Africa's Standard Bank. It's similar to apps used in the U.S., such as LevelUp or Square.

I used a U.S. credit card to purchase a prepaid debit card from a local bank that has a partnership with my U.S. bank, saving on foreign transaction fees. I entered its details into SnapScan, then walked into the nearest Standard Bank branch, went to a SnapScan terminal, held up my phone to the screen with the app open, entered my desired amount and voilà ... out popped a pile of local banknotes.

I avoided having to use my vulnerable U.S. ATM card entirely. Afterward, I was able to obtain cash or even make purchases directly using this simple, secure cellphone app.

This illustrates the secret to safe banking abroad: "cloud computing." That's a fancy term for large "farms" of remote servers that allow centralized data storage and processing for a variety of always-available internet-based services, like the one I used. Cloud computing has created endless opportunities for innovative, competitive software companies to develop and deploy new smartphone apps for paying for goods and services, without having to own and run their own expensive server farms.

Often called "e-wallets," these financial smartphone applications allow you to avoid the obsolete card technology still used by most U.S. banks when transacting abroad. They are actually safer than credit cards, including the hack-resistant chip-and-PIN cards used abroad. And as I'll explain, e-wallets have the happy side effect of often reducing or entirely eliminating costly foreign transaction fees (for you) and credit card terminal fees (for merchants).

Freedoms the Banks Will Hate — But You Will Love

For generations, most retail banks around the world have stored our money and/or given us lines of credit and charged us fees and interest. They've also supplied the means by which we access our money and our credit — debit and credit cards.

This amounts to a double-dip. That's because the systems required to use debit and credit cards — such as MasterCard and Visa — were created by the banks themselves. Merchants who accept bank-issued cards must pay fees to these networks.

These payment systems still rely mainly on telephone lines because they were built before the internet. A critical element is the "terminal" that accepts your payment card at checkout — the "point-of-sale" (POS). They are usually provided by the bank to the merchant for a fee.

The payment processor (e.g., Visa) charges the merchant a fee every time you use a POS terminal to make a purchase. A portion of these "swipe fees" is shared with your bank and the merchant's bank. Busy merchants can generate thousands of dollars in fees every day. They're highly unpopular and have generated numerous lawsuits, but they're central to the business model of current U.S.-style retail banking systems.

There is another problem — besides the fees — with these archaic networks. With millions of terminals in use, changing technology to something safer — say chip-and-PIN instead of magnetic stripe — is a wildly expensive proposition. Card processing companies expect merchants to pay for new terminals, but merchants don't want to. Resistance to mass replacement of merchant POS terminals is the main reason the U.S. lags so far behind the world.

But as we all know, the security weaknesses of magnetic-stripe technology to store card data has been highlighted in POS system breaches at major U.S. retailers, including Neiman Marcus Group, Michaels, Lowe's, SuperValu, Albertsons, Target and Home Depot. That's created an incentive for change.

It's this combination of unpopular fees and restrictive, insecure technology that's created a gap for alternative

smartphone-based payment systems that bypass the card terminals altogether — the key to safe transacting for you. A merchant can acquire a generic QR code-reader and connect it to the internet, or even use their own smartphone or tablet to accept payments.

Your payment is charged to your own debit or credit card, which they set up in the payment app as I did when I used SnapScan while in South Africa.

Daily, weekly or monthly, the payment app company transfers funds to the merchant — all without card swipe fees, saving the merchant — and you — lots of money. The app I use in the U.S., LevelUp, gives me a 7% discount on all purchases, for example. That really adds up.

So why, then, would a bank invest in a smartphone payment app that undermines its own traditional business model? One longtime friend of mine in the banking industry put it to me this way:

“We recognized that we could make more money by attracting clients with advanced front-end banking services than taking fees from traditional POS machine transactions. We lose a bit on the old-fashioned system, but we more than make up for it by people banking with us so they can use our app for free.”

Almost everyone, everywhere has a smartphone now, so it makes sense for banks everywhere to piggyback off that consumer trend.

But Is It Safe?

The question you’re probably asking right now is whether this sort of system is safe, given the dangers lurking on the internet — which is where banking is moving, after all. The answer is: It’s safer than using a traditional debit or credit card. A lot safer.

That’s because the payment apps I’m going to recommend don’t actually store your debit/credit card details on your smartphone or on their own servers. Instead, they use the sophisticated encryption technique I mentioned above, called tokenization.

This involves converting your Primary Account Number (PAN, aka your card number) into a unique, randomly generated sequence of numbers and/or alphanumeric characters. This “token” is stored in a special part of your smartphone’s memory that’s impossible to decode — even the phone’s manufacturer can’t read it.

When you make a purchase with a payment app, your card information is “tokenized,” encrypted and sent to the bank, which decrypts it and authorizes the transaction. The token is never stored by either the merchant or the bank. This avoids exposing your real card information to theft. You, the customer, never notice the difference in the way transactions occur.

Of course, all this encryption magic doesn’t do you any good if your smartphone is lost or stolen ... but if you have (a) a passcode to secure the device, (b) a PIN for opening your payment app and (c) a way to “wipe” all the data from your smartphone remotely, as I do with Apple’s “Find My iPhone” app, you are as protected as you can be.

Of course, there are certain privacy risks — distinct from financial risks — that come from using cellphones and their apps. Some apps can compromise your location and other private data, so it’s important to use those that don’t — as I’ll discuss below.

Saving You Money

Besides convenience and safety, cellphone-based transacting abroad can save you a lot of money. Consider the fees when you use a conventional ATM card outside the U.S., or even inside it, when using another bank’s ATM:

- **Flat fee from your bank:** This is a fixed fee that your bank charges for using ATMs outside of its network. These fees usually vary between \$2 and \$5.
- **Flat fee from the foreign bank:** You also have to pay a fixed fee to the foreign bank which owns the ATM you're using. This again is usually in the range of \$2 to \$5.
- **International transaction fee:** Instead of a fixed fee (or in addition to it), your home bank may charge a percentage fee for foreign withdrawals. These range from 1% to 3%.
- **Currency exchange fee:** The ATM interbank network — like Plus (operated by Visa) or Cirrus (MasterCard) — will also take a 1% cut.

Now consider the method I used. I bought a prepaid foreign debit card in a single transaction using my foreign credit card, on which I paid an international transaction fee of 1%. I then loaded its information into the local payment app, and from that point on, I paid no foreign transaction fees. Of course, I wouldn't have paid any such fees if I had used the foreign prepaid debit card directly, but then I would have lost the extra security of encrypted tokenization.

Payment Apps: Solutions You Can Use Abroad

The wave of the future — and of the present in much of Europe, Asia and Africa — is therefore a hybrid system in which banks provide money-storage and credit facilities, but independent application developers provide secure, internet-based POS systems that largely bypass traditional credit card processors such as Visa and MasterCard.

This technology is growing globally at a breathtaking clip. As of 2016, China had accounted for 58% of mobile-based commerce conducted across the markets researched by Euromonitor International. China's biggest mobile-payment service provider, Alipay, is looking to replicate that success abroad, aggressively expanding into Australia, Germany and the U.K. It recently announced deals with Verifone and credit card processor First Data Corp to propel its push in the U.S. Alipay has a goal of expanding its base from 450 million to 2 billion users within the next 10 years. And that's just one company!

The ease with which merchants can access these payment systems — often simply by downloading them to a tablet or laptop computer — means they can accept multiple payment systems in their store or restaurant, no matter how small. And since customers can simply download the app and set it up while they're on the go, any of us can access them as needed, recharging them with local prepaid debit cards, as I did.

So you're thinking about going abroad ... and you're wondering which app you need, where to get it and how to set it up and use it. Let's review your options. Remember, I'm talking here about solutions that allow you to turn your vulnerable physical magnetic-stripe cards into virtual payment systems that require no card to be present.

As I discovered, the reality is that in most countries outside the major markets of North America, Europe and Asia, you will need to use a local smartphone app to make payments. I was able to do this with SnapScan in South Africa using my Apple iPhone. As I explained, however, I was only able to do so because SnapScan allowed me to load a local prepaid debit card into the app. That might not always be an option in every country. In such cases, you might want to stick with cash or ideally, as long as your U.S. bank has issued one, your chip-and-PIN card. Of course, if you have a bank account in a foreign country, you can probably use a compatible local app with their bank cards.

When using a foreign payment app, the key is to ensure that it uses tokenization to encrypt your card details. At the moment, the only sure way to know that (other than to research the app yourself) is to see

whether it is compatible with all types of smartphones. If it is, it's probably not secure. Token-based apps only work with iPhone 6 (or later) and recent Android phones.



Tool No. 7: The i-Account

Throughout this report, I've written as if the question of where your money is ultimately stored is not a major issue. Only in the case of payment apps or countries that don't work with U.S.-based accounts does this become an issue, in which case I've recommended using a foreign prepaid debit card as a work-around.

But the ultimate source of your banking facilities does indeed matter, as we all know. For reasons of privacy, wealth protection and overall peace of mind, having at least some of your money in a secure offshore bank account that you can access via payment apps — or directly — is essential.

That's where the i-Account is the essential linchpin of your offshore transaction strategy. The i-Account is based on one of the world's safest and most private banking jurisdictions, Hong Kong. Funds are stored in a Chinese bank with the highest possible global ratings, far beyond the prying eyes of Uncle Sam. Even though you must report i-Account balances if you fall under FATCA and FBAR thresholds, the actual data related to your overseas transactions is entirely inaccessible to the U.S. government.

That fact alone makes the i-Account my preferred choice for the debit card I'd load into Apple Pay or another app for use when traveling. Besides the intrinsic security of your i-Account details, tokenization means even those i-Account details will be completely secure.

But there's another huge advantage to the i-Account that basically makes it the ultimate deal for global travelers like you and me.

You can hold your i-Account funds in any one of 22 currencies (USD, EUR, JPY, GBP, NZD, CAD, AUD, SGD, HKD, CHF, CNY, PHP, NOK, DKK, SEK, CZK, TRY, HUF, BGN, RON, IDR and TWD), with more on the way. You can exchange among these currencies instantly with no added fees, at competitive rates. So instead of having to pay your U.S. bank currency exchange fees when using a payment app, either on every transaction or when purchasing a foreign prepaid debit card, you can simply load your i-Account with the appropriate foreign currency — say, euros — and away you go ... no currency-conversion costs at all.

If you would like more information about opening and using i-Account, you can go to <http://www.i-Account.cc/>. There you will learn more about funding your i-Account, the currencies available and even uses for corporate accounts.

Be Safe

So there you have it ... seven free tools for keeping your information private and safe in the digital age. These strategies are still expanding rapidly across the globe and haven't reached everywhere yet, but thanks to Banyan Hill, you'll be ready before almost everyone else.

Kind regards,

A handwritten signature in black ink, appearing to read 'Ted Bauman', followed by a long horizontal line.

Ted Bauman, Editor
The Bauman Letter



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 expressly forbids its writers from having a financial interest in their own securities or commodities recommendations to readers. Such recommendations may be traded, however, by other editors, its affiliated entities, employees, and agents, but only after waiting 24 hours after an internet broadcast or 72 hours after a publication only circulated through the mail. Also, please note that due to our commercial relationship with EverBank, we may receive compensation if you choose to invest in any of their offerings.

(c) 2017 Sovereign Offshore Services, LLC. All Rights Reserved. Protected by copyright laws of the United States and treaties. This Newsletter 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)