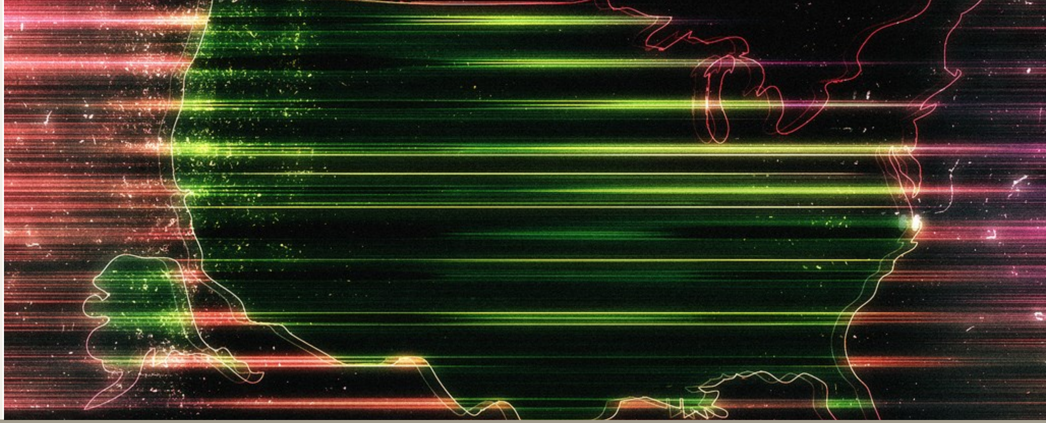
in this issue >>> *V.1.14*



TOUCHPOINT
INTERNATIONAL DEVELOPMENT GROUP, INC

A Bi-Monthly Snapshot into Emerging Threats and Trends

Digital Update

current topics >>>

In the News:

- [The Limits of SMS for Two-Factor Authentication](#)
  - Krebs on Security
- [U.S. Gets its First Chief Information Security Officer](#)
  - Naked Security
- [New Mac OS Updates Patch Same Vulnerabilities as iOS 9.3.5](#)
  - Ars Technica
- [PC and Mac Lock Screens Are Bypassed with Ease](#)
  - Ars Technica
- [Two New Critical Android Bugs Affect Millions of Devices](#)
  - Ars Technica

VeraCrypt V 1.18

Free FDE for Windows is Back!

A few issues ago, we reported that Bitlocker is the encryption option of choice for PCs running Windows 10 or later. Windows 10 uses a UEFI firmware instead of the older BIOS, and versions of VeraCrypt have not—until now—supported UEFI machines. This is a sad state of affairs because full disk encryption is the best form of encryption you can use to protect the data on your computer. Thankfully this has recently changed.

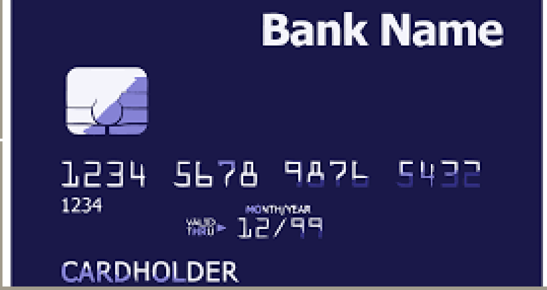
The most recent version of VeraCrypt, version 1.8, now supports full-disk encryption for Windows 10 computers with UEFI. To full-disk encrypt your machine you will need the to install VeraCrypt 1.18 and have a CD/DVD burner and a CD. This is to create the VeraCrypt Rescue Disk. Open VeraCrypt and click “Create Volume”. Choose “Encrypt the system partition or entire system drive”. Next, select “Normal”.

On the next screen you will be given a choice of encrypting the Windows System Partition, or the entire hard drive. We recommend encrypting the entire hard drive, if that option is available to you. If it is not, this may mean that there is only one partition on your hard drive. On the next screen you will be asked to choose Single Boot or Multi-Boot; most users will choose single boot. Multi-boot is for users who have more than one operating system installed on their hard drives.

You will be asked to create a password and then you will be asked to create a VeraCrypt Rescue Disk. This does DOES NOT contain your password—it is a backup copy of important encryption information in case your computer’s encryption becomes corrupted. You should store this disk in a safe place. Once you have burned the rescue disk your computer will reboot to verify it works with the encryption. After it has done so successfully you can begin encrypting your computer.

Encrypting your machine will take some time. If you need to interrupt the process you can by clicking the “Defer Encryption” button. When you restart your computer you can resume the encryption process. We strongly recommend you full disk encrypt your computers. For more information and to download VeraCrypt visit **https://veracrypt.codeplex.com/**.

set the stage >>>



Mask Your Credit Card with Blur

If you have attended any of our Identity Management training, you know that protecting your credit card information is important. Credit cards are routinely stolen when people use public Wi-Fi, when a merchant's databases are breached, or on forged websites. Once this information is stolen it can be used to make charges that you might be responsible for, or you might not, but cleaning up the mess is a hassle either way.

Fortunately, two relatively new services allow you to mask your financial information. The first is called Blur. Non-Standard Communications graduates know that we love Blur because it does a number of things. Blur allows you to mask your email address by creating randomly generated addresses that forward to your regular email account. They also have a phone masking function that forwards calls to your real phone number.

The masked credit cards function is the one thing Blur has that no one else does. Masked Credit Cards allows you to create credit cards that are essentially one-time-use. If you're about to make a purchase on a websites, you login to your account, go to "Masked Credit Cards" and create a new card for the amount of the purchase. Blur will charge your credit card for the amount (plus a small fee). You then give the merchant this credit card number, and any shipping name and address you like.

This card number will be worthless as soon as it has been processed by the merchant. If the merchant's website is hacked tomorrow, that's ok. The card number has no value and cannot be used to make purchases.

The downside to Blur: to access the Masked Credit Card feature you will need a premium account. Blur costs $39.99 annually, or $79.95 for three years. This is a service we use on a daily basis. For more information visit Blur's website at **https://abine.com/index.html**.

The easy button >>>

Pay With Privacy: Privacy.com

Though we like Blur for its rich feature set, we don't like that it is a paid service. Fortunately a new service has come along that offers similar privacy enhancing payment services and it is completely free. It is called Pay with Privacy and is available online at **https://privacy.com**. Pay with Privacy works a little different than Blur. First it requires that you link a bank account rather than a credit card. This will be the funding source for your future Pay with Privacy cards.

Your Pay with Privacy account allows you to create multiple credit/debit cards that draw from your bank account. Each of these may be set up with a number of security features including Single-Merchant, Burner Card, and Spending Limit. Single-Merchant cards will "lock on" to the first merchant with which they are used, and cannot be used anywhere else. This would be good in cases like your phone bill. You can leave the card open, but it can only be used with your cell provider. Burner Cards will expire two minutes after the first purchase is made with them. These are great if you are signing up for an online service that will try to bill you on a recurring basis when you only want a one-month subscription. Spending Limit cards are only valid for a certain amount. All of these options give you flexibility and help make the number worthless should it fall into the wrong hands. If one of the numbers is stolen you have the option to pause the card, or completely close it. Closing a card is permanent and cannot be undone.

Our one complaint with Pay with Privacy is that it is currently invitation only. Visit **https://privacy.com** and click "Request Invite". Give them your email address (or a Blur Masked Email address) and wait for your invitation to come in. We have had to wait several weeks for invitations but the wait is well worth it. Once you have an account it is completely free.

Upcoming Events:

Ft. Gordon Cyber Security & Tech Day

19 October 2016, Augusta, GA

Law Enforcement Intelligence Units

1-5 May 2017, Bloomington, MN

For more information go to
www.tpidg.us

ProtonMail Premium Plans

Expanded Features

We have previously written about ProtonMail here in the Update. If you have attended our Non-Standard Communications Course you already have a ProtonMail account because it is one of the email accounts we recommend for use during the course. We have yet to address ProtonMail's new premium plans, however. These plans are paid and come with some excellent expanded features. Though no one likes paying for email your money goes to support ProtonMail and helps keep development in motion.

The baseline premium plan is called ProtonMail Plus. This plan upgrades your account from 500 MB to 5 GB of storage. The smaller, free email inboxes fill up quickly. Having the extra storage is extremely helpful if you are using ProtonMail as a full replacement for a mainstream email service.

ProtonMail Plus also gives you five email aliases—you can make these email addresses anything you want and they will forward to your regular inbox. When you reply from an alias address, the recipient only sees the alias address and not your regular ProtonMail address. In the last issue we talked about using usernames as a security measure and this lets you do just that. You can setup your account with a long (up to 40 characters) username and never give it out. Instead you can use your aliases as the email addresses that you give out to friends, family, and businesses. If you are using an email masking service like Blur each one of your aliases and have truly unlimited addresses at your disposal.

The basic ProtonMail Plus plan also allows you to add one custom domain. If you own a domain for business purposes this is extremely helpful. Or if you don't like giving out "@protonmail.com" email addresses because it elevates your profile you may wish to purchase a domain that you can use for your email. Once you have a domain you can create an unlimited number of email address, like "john@customdomain.com". Again, all of these forward to the same inbox so you only have to login once to check all of your mail.

ProtonMail's premium plans offer a baseline package and then let you pick and choose the features that are most important to you. If you want to add more storage you can in 5 GB increments. If you want more alias addresses you can add these in increments of five. If you want more custom domains you can add them. Each item only increases the overall cost slightly.

If you are looking for a sole-source email solution you should definitely give ProtonMail a close look. Now that apps are available for iOS and Android phones ProtonMail is just about as convenient as anything else. And just like your regular ProtonMail account, all of the information stored on your Plus account is encrypted with PGP. This means that no one—not even ProtonMail administrators—have access to your email.

coming soon >>>

In Future Issues...

Synology NAS

Email Forwarding Services Compared

- *33Mail*
- *Blur*
- *Not Sharing My Info*

Lock Screens

Don't Rely on Them!

A new attack was revealed this week that can bypass Windows and Mac lock screens. The attack is executed through a malicious USB flash drive. Researchers reported being shocked by how easy it was. This is bad news for those of us that work in offices and frequently leave our computers powered on and logged in but protected by the lock screen. The lock screen provides virtually no protection from someone with physical access to your device.

Instead, we recommend full disk encryption. Our cover story in this issue is about VeraCrypt being capable of encrypting Windows 10 disks. Now that free full disk encryption is available for Windows, Mac (FileVault), and Linux (LUKS, VeraCrypt) computers, there is little excuse not to use it. Bitlocker is also a worthy alternative that we have advocated in the past but the $100 price tag to upgrade from Home Edition is understandably a show-stopper for most.

Your lock screen is fine for leaving your computer to run to the restroom, (as long as you are in a safe space) but you shouldn't rely on it for much more than that.