in this issue >>> *V.1.18*

TOUCHPOINT
INTERNATIONAL DEVELOPMENT GROUP, INC

A Bi-Monthly Snapshot into Emerging Threats and Trends

Digital Update

current topics >>>

In the News:

- **Web of Trust Add-On Sells Your Browsing Data: Uninstall NOW!**
  - Lifehacker Security
- **You Can Now Use LastPass on Multiple Devices for Free**
  - Lifehacker Security
- **Windows "Patch Tuesday" Releases Numerous Critical Bug Fixes**
  - Naked Security
- **Fix for Critical Android Bug Absent in November Patch Release**
  - Ars Technica
- **How to Block the Ultra-Sonic Signals You Didn't Know Were Tracking You**
  - Ars Technica

Backup Basics

Why YOU Should be Backing Up

Chances are good that most readers of the Digital Update already know they should be creating backups of their computers and phones. This issue of the Update is going to talk about backups and some backup utilities. Before we get into all that, we want to talk about why backups are so important.

Whether it is years of family photos, thousands of business invoices, or reams of reports, data loss can be disastrous to individuals and organizations. Data recovery is extremely expensive and is not always feasible. Most of us will go many years without experiencing significant data loss, but the odds are not on your side. Below are the top reasons you may lose your precious data.

Hardware failure. This is the most common cause of data loss. Legacy spinning hard disk drives (HDDs) are extremely prone to this. A hard drive is comprised of parts moving at speeds of up to 7,200 RPM. The slightest amount of moisture or smallest speck of dust can interfere with the extremely tight tolerances and render an HDD inoperable. You should also consider normal wear and tear: a hard drive will only survive for a finite life cycle. If you are slow to upgrade to a new computer it is possible to outlive its storage device.

Loss or theft. Though unlikely, we cannot overlook the potential for losing a device. If your device is lost or stolen so is all your information—unless it was backed up properly. Loss could occur as the result of leaving your phone in a taxi, your house being burglarized, or any number of other reasons.

Regional disaster. If you live in an area prone to tornados, floods, earthquakes, hurricanes, or other natural disasters, take note. Large-scale disasters make up the second leading cause of data loss. Your house or office may be destroyed or inaccessible for months at a time, and flooding or other damage can render your devices unusable.

House fire. It is estimated that one in four Americans will suffer a house fire during their lifetime. This traumatic time is complicated by loss of your computers, access to online accounts, digital copies of insurance records, and personal items.

Losing data is possible through a number of scenarios. Regardless of the reason you should prepare for this eventuality now. After you have lost data it is too late to prepare for it. In coming editions of the Update we will discuss some tools that will allow you to create a comprehensive backup system for your most important information.

set the stage >>>

Email Masking: NSMI

We talk about Protonmail a lot in the Update. We usually focus on Protonmail's security features, but the premium versions offers some excellent privacy benefits. Protonmail "Plus" and "Visionary" plans offer alias email addresses as part of a package deal that includes increased storage space and the ability to use a custom domain.

The ProtonMail Plus package offers 1 GB of storage, one custom domain, and five alias Protonmail addresses at $5.00/month or $48.00/annually. Additional alias addresses can be purchased in blocks of five for $1.

Protonmail aliases work like this: you create a new Protonmail address (@protonmail.com or @protonmail.ch). You can give this address out to anyone you like. All mail sent to this address will be forwarded to one single inbox. When you receive an email address to an @protonmail.com address and click reply, by default you will reply from the address it was sent to. You can also reply from any of your other Protonmail addresses if you wish to do so. Simply click the drop down beside the "From" line, and a list of all your available addresses will appear.

Protonmail's implementation of email masking is something we wish we had in other mail services. It is extremely easy to use and robust but there are some issues with it. First it is not free, as are all of the other services we have mentioned in the email masking series.

The other big downside is that Protonmail premium aliases are permanent. They will always count toward your allotment of aliases and cannot be deleted. This means that if one of them gets "burned" or you simply don't desire to use it anymore you will still be paying for it. You can turn it off so you will no longer get mail from it, but you can never completely delete it.

If you are looking for the most robust email forwarding solution possible check out the Protonmail premium plans at **https://protonmail.com**.

Upcoming Events:

Law Enforcement Intelligence Units

1-5 May 2017, Bloomington, MN

National Technical Investigators' Association Annual Training Conference

July 12-23, Tampa, FL

The easy button >>>

Ubiquiti Video Surveillance

The Ubiquiti UniFi UVC-G3 is a 1080p indoor/outdoor IP surveillance camera with audio and infrared capabilities. It is able to be mounted on the wall or on a pole with a special mounting bracket, making it very versatile with placement. The camera shoots in full HD (1080p) and has a very decent adjustable frame rate of 30 FPS. The camera is powered by 24v PoE (Power over Ethernet) via a single Ethernet cable for both data and power, making cable management easy. You can supply power to it with the Ubiquiti ToughSwitch (or something similar) or with the injector that is supplied with the camera.

As with all Ubiquiti cameras, you can either manage the camera as a standalone camera or you can integrate it into UniFi, a video surveillance system designed and maintained by Ubiquiti.

If you choose the standalone route, you have a constant live view that can be viewed on the router's admin page and you have RTSP (Real Time Streaming Protocol) capabilities. Ubiquiti allows you to stream audio and video in real time to wherever you want to view or record it (it works very well with VLC player). The only issue with the way Ubiquiti integrated RTSP into the camera is they did so without any sort of authentication. So basically anyone with the address of the camera can also stream video and audio in real time without a username and password. This is not ideal, but as long as you keep it on a local network segregated for the purpose of recording video and audio only, you should be fine.

The other option is UniFi which we will review in an upcoming issue because it entails a lot and deserves a detailed review. Overall, the camera is spectacular for home/office surveillance. Full HD, night vision, PoE and more from this little Ubiquiti camera makes it makes it worth every penny. For additional info or questions, contact admin@tpidg.us

Cloud Storage

Offsite and Out of Mind

Offsite backups are those backups that are stored in a different location from your primary device. This can range from a hard drive stored down the street in a safe deposit box to information stored in a cloud storage account. There are some major benefits to offsite backups that you should be aware of. Unfortunately there are also some security and privacy concerns around storage that you should also consider.

The major benefit of an offsite backup is that it protects you from disasters like residential/commercial structure fires, burglary, and regional disasters. If one of these things occur, you have a backup in place that is distributed among cloud servers that are unaffected by the disaster. As soon as you have an internet connection and working device you can begin recovering your data.

The major disadvantage of cloud storage is that your documents, photographs, and other files may potentially be accessed by the storage provider. This is commonly the case with mainstream providers. Services like Dropbox explain clearly in their privacy policies that they can access your data. Some, like Google Drive, further explain that they will access this data to serve you directed advertising content. Though these services may be secure they are lacking when it comes to privacy.

Regardless of what cloud provider you use you should employ some security best practices to protect your account. We recommend the following best practices:

Random username: We have discussed this in previous editions of the Update, but your username should not be a common-knowledge email address or information that is easily guessable. This is your first line of defense for any online account.

Long, strong password: Of course we always recommend a strong password. In this instance you may wish to use one that you can remember and manually enter. If your primary computer is lost or destroyed you may no longer have access to your password manager database and need to get into your cloud storage account without it.

Two-factor authentication: As with any other online account, two-factor authentication offers an orders-of-magnitude increase in security and should be employed.

Client-side encryption: Regardless of what provider you choose to go with, we recommend encrypting your files locally before uploading them. There are a number of applications that you can use to do this and we will discuss a couple of our favorites (see sidebar). Even if the service is extremely secure and respects your privacy there is always the risk of data spillage through a hack.

coming soon >>>

In Future Issues...

Synology NAS

Local Backup Utilities

Mailfence

Client-Side Encryption

Protect Your Data in the Cloud

Two of our favorite client-side encryption programs for cloud storage applications are CryptSync and Cryptomator.

CryptSync: CryptSync is available for Windows. It allows you to create an original folder and a destination folder. It will duplicate the contents of the original folder into the duplicate. As you modify the contents of the original folder by adding, deleting, or editing files, CryptSync will apply these changes to the destination folder.

This works extremely well with cloud storage. Define your important files as the "original" folder and your cloud upload location as the "destination". The best feature from a security standpoint: the contents of the destination folder are encrypted locally using AES-256. For more information visit **http://stefanstools.sourceforge.net/CryptSync.html**

Cryptomator: Cryptomator is similar to CryptSync but is optimized for Mac. We also like that this application is available from the App Store which means it is signed with an Apple signing key.

Cryptomator requires no registration, and encrypts each file individually with AES-256. Simply create a vault in Dropbox, Google Drive, or anywhere else and Cryptomator will encrypt the files you add to it.

Cryptomator is free and fully open source. For more information visit **https://cryptomator.org/**.