TOUCHPOINT
INTERNATIONAL DEVELOPMENT GROUP, INC

A Bi-Monthly Snapshot into Emerging Threats and Trends

Digital Update

CURRENT TOPICS >>>

[Appeals Court: Lawsuit Over Wrong Info on Spokeo Should Move Ahead](#)
-Arstechnica

[Leak of >1,700 Valid Passwords Could Make The IoT Mess Much Worse](#)
-Arstechnica

[US Debit Card Compromises Up 39%: FICO](#)
-Dark Reading

[Hacker Releases Decryption Key for Apple's Secure Enclave Firmware](#)
-Bleeping Computer

CURRENT COURSES >>>

ESSR

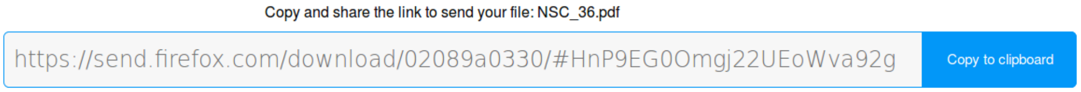
The Electronic Security and Signature Reduction (ESSR) course teaches students how to evaluate, manage and eliminate their digital signature. Students will learn how to secure data at rest and data in motion through open source programs and phone applications. Students will leave knowing how to "research" themselves and understand what the Internet has on their life. They will then learn how to manage or eliminate their online profile.

Firefox Send

Encrypted File Transferring Service

Recently, Mozilla started a new test pilot project they named *Send* that allows anyone to upload a file to be shared securely with anyone in the world. Send is a completely open source project run by a small group of developers. With Send, you can upload a single file up to 1GB in size and it gives you a unique link that you can send to whoever needs to download the file. The file only stays on the server until downloaded or 24 hours, whichever comes first, so if you had multiple recipients you would have to upload the file multiple times and send out multiple unique links. It is intuitive and very easy to use even for the least qualified internet user. It's as simple as: browse for your file or drag and drop, wait for the upload, and then send someone the auto generated link. The speeds are quite impressive as well, much better than most file upload sites especially considering the file is being encrypted at the same time.

Send uses the JavaScript Web Cryptography API which uses AES in GCM mode to encrypt while also ensuring file integrity. Because they are using JavaScript to perform the encryption, this means that just like ProtonMail, everything is encrypted client side and only the encrypted blobs are sent back to the server. This also means that the uploader needs to have exclusive access to the key as well, so no one else can unencrypt the encrypted file. Since the uploader never set a password or key, it needs to be generated. The way that Send does this is it first generates a secure password, encrypts the file with it, then submits it to the next page and appends it to the end of your unique link (pictured below). The file id is the first set of letters and numbers and the key starts after the # in the link. It is very important that this link be treated just like a password. This is only going to be secure as the means you use to send the link, so use trusted encrypted messaging platform (ie. Signal, Wire, ProtonMail). An attacker could easily intercept an unencrypted message, download the real file, upload his file and send the message off with his link instead of yours. This is obviously worse case scenario and highly unlikely, but it all depends on your particular threat model.


Copy and share the link to send your file: NSC_36.pdf

https://send.firefox.com/download/02089a0330/#HnP9EG0Omgj22UEoWva92g

THREATS AND VULNERABILITIES >>>

You Do Not Belong In Your Passwords

How many people did you invite over on your birthday? How many people saw your birthday on their Facebook timeline? How many organizations have you freely given your birthdate to? Make sure you count very carefully because this is how many people can unlock your phone right now. If you are the large majority of users that include personal information in your password or PIN, you should probably go change all of your passwords right now. A password was designed to be secret and something only you would know, but if you are using personal information such as: your birthdate, your SSN, your address or anything else personally identifiable, you aren't using a password, you are using public record to protect your device. If anyone gets access to any of your devices, personal information is the first thing they are going to try to unlock your device. This goes for online accounts as well, with a device PIN, an attacker would first need to gain access to your device. With online accounts, an attacker doesn't even have to leave their bedroom, they can keep going at your account from the comfort of their bed. An attacker could do an in-depth OSINT search into your life, figure out your full name, birthdate, home address, phone number, email address, kid's names, pet's names, hobbies and interests, and any other personal information. They could then use all of that information to generate a dictionary list of every possible password you could ever make out of personal details about yourself. This could be a very simple letter-only password list or it could be complicated with numbers and symbols. For instance, if my birthdate is January 1st, 1970 and my pet's name is Scooby, a couple passwords may be:

Scooby70 **Sc00by70** **Jan0170**

This is not a manual process either, a skilled attacker has either written their own program to generate these lists or uses a freely available program to generate these lists. Touchpoint has verified these techniques through helping local law enforcement lawfully unlock devices.

EVENTS >>>

Air, Space & Cyber Conference

Sep 18-20 2017, National Harbor, MD

Techcrunch Disrupt

Sep 18-20 2017, San Francisco, CA

Microsoft Ignite

Sep 25-29 2017, Orlando, FL

READER QUESTIONS >>>

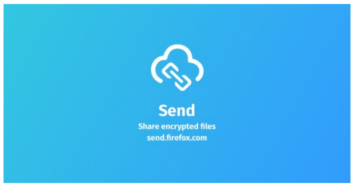
Have a specific **question** you would like us to answer?

Have a suggestion for a **topic**?

Want to **contribute** to the digital update?

Let us know at
digitalupdate@tpidg.us

MAIN ARTICLE CONTINUED >>>



Firefox Send

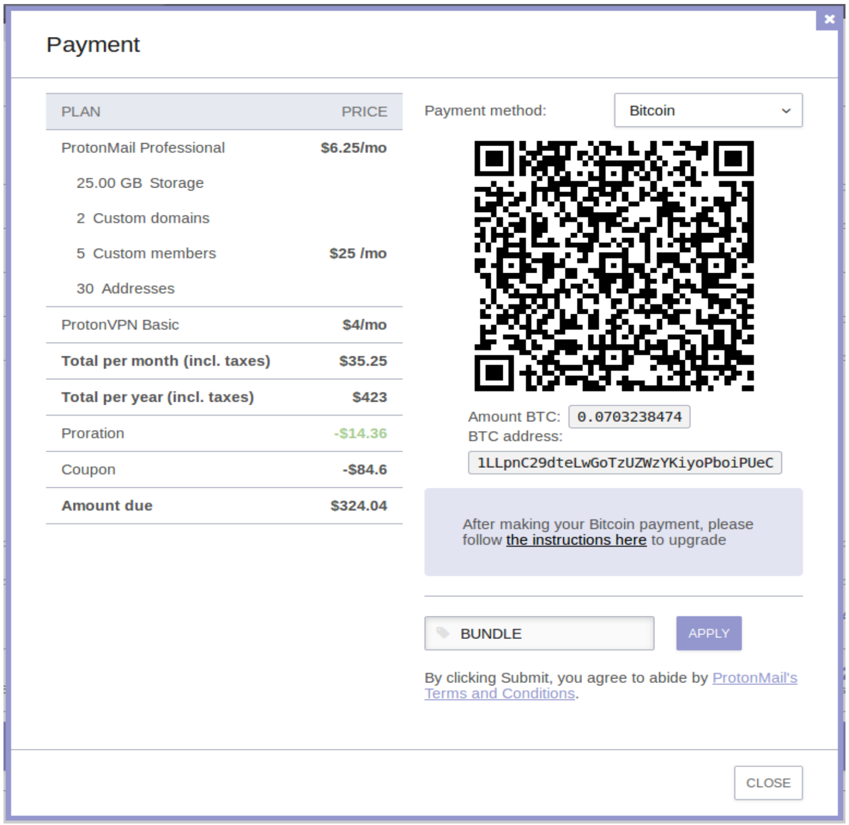
At no point does the server ever see the contents of your file, but it can see a few things that may make you a bit uneasy using it. First and foremost, it collects the name of the file. This could either be the worst thing in the world or it may not matter depending on what you name the file. If you name the file something generic such as report.xlsx, then it doesn't matter either way, but if your filename is something specific such as john_smith_999-99-9999.pdf, you probably don't want to upload it to Send. Just because a file's contents is encrypted doesn't mean it can't still give some identifying information. There is an active plan to encrypt the filenames as well, but in the current build, filenames are passed to the server in plaintext. Send also collects various other metadata including the following: file size, how often you upload files, file transfer errors, and file type. Similar information is also stored in your browser. Until recently, Send was also taking hashes of uploaded files before upload and storing those hashes for testing purposes and to be checked against known malware hashes (similar to what Dropbox does). Thankfully, they completely did away with this last month.

Another concern is that their hosting provider is AWS (Amazon Web Services) and the fact that they have their own privacy policies and terms of service that are completely separate from Send and Mozilla. If Send was subpoenaed, they may be able to say they can't help and the files were already deleted, but what happens when AWS gets subpoenaed? Amazon could cooperate with law enforcement or a foreign government by running a disk recovery software or by saving copies of the encrypted files as they are uploaded. Yes they are still encrypted, but if they have access to the files and they know the filenames, the size and the file type of each file, they can target specific files and it's only a matter of time before they gain access. Of course, this is assuming there were enough resources behind trying to unencrypt a few files. Send is still a part of the Mozilla TestPilot program and is under active development and we hope to see major improvements on the privacy side in the future.

ProtonMail Updates

Bitcoin and ProtonMail Professional

At long last, ProtonMail now supports payments through Bitcoin. You can now use all of your stockpiled bitcoins to purchase a paid plan or you can just donate to the cause. This is a huge step for Protonmail as masked credit cards and prepaid cards don't tend to work when purchasing the paid plans for fraud reasons. With bitcoin support, you can acquire a paid email service 99% anonymously.



Payment

PLAN	PRICE
ProtonMail Professional	$6.25/mo
25.00 GB Storage	
2 Custom domains	
5 Custom members	$25 /mo
30 Addresses	
ProtonVPN Basic	$4/mo
Total per month (incl. taxes)	**$35.25**
Total per year (incl. taxes)	**$423**
Proration	-$14.36
Coupon	-$84.6
Amount due	**$324.04**

Payment method: Bitcoin

Amount BTC: 0.0703238474

BTC address:

1LLpnC29dteLwGoTzUZWzYKiyoPboiPUeC

After making your Bitcoin payment, please follow the instructions here to upgrade

BUNDLE

By clicking Submit, you agree to abide by ProtonMail's Terms and Conditions.

Also in the month of August, ProtonMail has fully rolled out multi-user support for organizations with their ProtonMail Professional plan. This allows organizations to bring over their domain name and add all of their employees to that domain, giving every user end-to-end encryption on all of their emails. It is still possible for your organization to monitor employee's emails through ProtonMail's crypto-magic just in case a disgruntled employee leaves and doesn't give access to their email. ProtonMail Professional also includes an option for a catch-all email. More information can be found on the ProtonMail blog:

https://protonmail.com/blog/

Software Updates

We preach updates in every class, so here's a list of security software updates for the month of August accompanied by sha256 checksums.

TOR Browser Bundle

Version: 7.0.4

Released: August 8th, 2017

torbrowser-install-7.0.4_en-US.exe

b1f1ead0d77381180e1fb5519a9cf67f0337956ea466c805be3f2bdda7c03491

TorBrowser-7.0.4-osx64_en-US.dmg

0a227d179cdd1096c877f9836097eb38ed554fbae6657753a72690a183e2766d

tor-browser-linux64-7.0.4_en-US.tar.xz

7d09fdf1dad4657de16556deecf497253f8564bdbe85a9e7fa00f97bb6351f9e

TAILS Live ISO

Version: 3.1

Released: August 8th 2017

tails-amd64-3.1.iso

0ef1c7d880308ee9f98c255b2658b75445cc84622eae2944a342dcc50cea71c7

Firefox

Version: 55.0.3

Released: August 25th, 2017

Firefox Setup 55.0.3.exe

b89bcd773c03f491b960e16a03fac4086791c5baebc162554a4ec56b33675621

Firefox 55.0.3.dmg

f755408409f00ba6842aba4e849f5724883e974306a52fec7a12e4ed7a1b4006

firefox-55.0.3.tar.bz2

f0fd11357de7250660f1a5c5b209c44de1d0f50bb1d3444dd2afad6b41e15b9d