in this issue >>> *V.1.3*

TOUCHPOINT
INTERNATIONAL DEVELOPMENT GROUP, INC

A Bi-Monthly Snapshot into Emerging Threats and Trends

Digital Update

current topics >>>

In the News:

- Certified Ethical Hacking Website vector for Crypto/Ransomware malware
  - Ars Technica
- Verizon Wireless; 1.5 Million Enterprise Customer Records Spilled
  - Krebs On Security
- Seven Iranians Indicted by Federal Grand Jury for "Campaign of Cyber Attacks" **- Ars Technica**
- Chinese National Pleads Guilty to Stealing US Military Secrets
  - Naked Security

Thirty-Day Security

Become Digitally Secure in One Month

Increasing your personal or operational digital security can be a daunting task. Even deciding where to start can be a major decision point, and each discrete task can have a myriad of second– and third-order effects. This is why Justin Carroll took the month of March to post a daily security task in what he called the "Thirty-Day Security Challenge".

The Challenge was designed with inexperienced users in mind. Rather than flood the user with complicated tasks, Carroll broke a myriad of security tasks into manageable bite-sized tasks that take only a few minutes out of each day. Users completing the challenge are doubtlessly far more secure than they were when the Challenge began.

The Thirty-Day Security Challenge was designed with inexperienced users in mind.

The first week of the Challenge focused on local system security. Users were instructed shown how to update their operating systems and applications, setup standard user accounts, review security and privacy settings, and scan with antivirus and antimalware applications. The second week focused on data in motion, with topics like securing your home Wi-Fi Network and internet browser. The third week of the challenge addressed some mobile device security topics and the fourth was geared toward identity management topics. Woven throughout the month was a recurring "Account Security Tuesday" which discussed changing passwords, adding two-factor authentication, and using unique usernames on your online accounts.

If you are looking for a well-rounded approach to becoming more digitally secure, or know someone who is, check out the Thirty-Day Security Challenge. Even though it is over the posts will remain on Justin's blog indefinitely.

THIRTY DAY SECURITY CHALLENGE

set the stage >>>

ID Management 101 *(Part 3 of 5)*

Part I of this series covered conducting self-background check. Part II talked about halting the spread of your data. Today we will look at removing it from the system

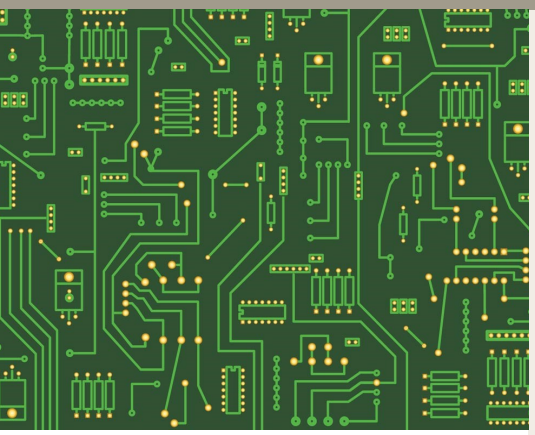
Start Controlling Your Own Information

It should be common knowledge in the U.S. that your personal information is a heavily traded commodity. Data has been called "the new oil" by Forbes.com. It is a multi-billion dollar industry, it is so valuable in fact that somewhere north of 90% of Google's $1.5 billion worth is owed to data collection and sales, and advertising. You can and should start taking this information back.

Your data is being used to make others millionaires, and it is getting you little more than a free email account. You can begin today by opting out of data collection. This is not an easy process, and it is never really finished. But the sooner you start, the less information that will be out there, and the better off you will be.

Take Back Your Data

An excellent resource for removing personal data from data brokers is a new website called StopDataMining.Me. This site offers a master list of opt-out requests for the various data brokers and advertisers. Data brokers do not want you to opt-out of their collection and monetization streams. Fortunately services like this can show you how. In the last segment our focus was "stop giving away your information". It is important to reiterate this now—going through the time and hassle of removing your information is futile if you put it back out there.



Upcoming Events:

-SOFIC 23-26 May 16
Tampa, Florida
-Blackhat 30 July-04 Aug 16
Las Vegas, Nevada
-NATIA 09-15 July 16
Seattle, Washington

For more information go to www.tpidg.us

The easy button >>>

Encrypted Email Update

If you are a graduate of our NSC or Data Protection courses then you understand the importance of protecting the content of your emails. Your email account contains a treasure trove of data about you. Mainstream providers scrape your personal emails for marketing data, and operational emails may

Our favorite encrypted email provider, ProtonMail, crossed a major hurdle this month. ProtonMail is now officially out of beta. What does this mean for your? Several things:

1. There is no longer a wait list to join ProtonMail.
2. ProtonMail now supports paid tiers that offer things like multiple aliases and custom domains.
3. ProtonMail has both iOS and Android mobile applications, both of which are free and available through the App Store and Google Play.

If you haven't used ProtonMail before, there are some good reasons to do so. Your emails are encrypted end-to-end between ProtonMail users. This means that no one—not even ProtonMail itself—an access your emails for any reason. Your attachments are encrypted, and you can encrypt emails to "outside" (non-ProtonMail) recipients. Best of all, basic ProtonMail accounts are totally free.

For more information and to set up your own ProtonMail account visit https://protonmail.com/.

Two-Factor Authentication

Online accounts are the Achilles' Heel of strong digital security. They exist online, are usually only modestly protected with a password, and are always under attack. Two-factor authentication is a robust option that increases their security by orders of magnitude. Enable it today!

So what is two-factor authentication (TFA)? Two-factor authentication (also called multi-factor, or two-step verification) is a protocol that requires you possess a physical token in addition to your username and password. In most cases the physical token is your smartphone. When you enable two factor authentication you will have to enter your username and password as usual. Before the account lets you in, it will also ask for a unique code. These codes can be sent via email, SMS, or an app that generates them in tandem with the website. SMS codes are the most prevalent.

How does TFA protect your account? Since each code is only good for one login, an attacker would have to get your username, password, and mobile device to get into your account. While it is possible, this is very unlikely.

Where can you enable two-factor authentication? Many sites support it, including Amazon.com, Google/Gmail, Microsoft/Outlook, Yahoo!, Facebook, Twitter, and many more. This list is not all inclusive; for a more comprehensive list of sites that support two factor visit https://twofactorauth.org.

Two-factor authentication may seem like a hassle and may take some time to get used to. However, the security it offers is significantly better than a password alone.

Virtual Private Networks

A virtual private network (VPN) is one of the most meaningful security measures you can take to protect your internet traffic. A VPN provides you both privacy and security by encrypting your connections.

Private and Secure

VPNs work by first establishing a connection with a remote server that is hosted by the VPN provider. This connection is then encrypted, creating a secure "tunnel" between it and your PC or phone. This prevents hackers, your internet service provider, and malicious Wi-Fi hotspot from monitoring your traffic.

A VPN also creates a strong privacy layer. Because your traffic appears to originate from the VPN's server, it protects your IP address which can reveal your true location, internet service provider, and other details a hacker could use against you.

Last week we talked about the Private Internet Access mobile app. Private Internet Access also works on your PC, Mac, and Linux computers, and is only $3.33/month if you purchase a full year's subscription. LINK

///// VULNERABILTY ALERT /////

In the past TouchPoint has taught Tutanota encrypted email in its Data Protection, Identity Management, and Non-Standard Comms courses (and we mentioned it in the last Digital Update). Today we are informing you of a vulnerability that affects users of the Tutanota mobile app. If certain settings are enabled on your mobile device your Tutanota password may have been stored in the cloud without your knowledge. This would have occurred if: you are using Android 6 (Marshmallow), have not disable cloud backups, and have stored your password in the Tutanota app.

Tutanota handled this vulnerabilitiy responsibly, alerting users as soon as possible. It has also issued an app update that patches this bug. If you meet the above criteria you should update the Tutanota app and change your password as soon as possible. We still believe Tutanota is an excellent option for a streamlined, end-to-end email option.

For more information on the bug and the app update please visit https://www.tutanota.com/

coming soon >>>

In The Next Issue

An Introduction to Threat Modeling
Exploits: Remote Access Tools
COMSEC: Wickr Me
Hardware Two-Factor Tokens
Austere Environment Wi-Fi: BRCK