

# Avoiding Fraud and Identity Theft by Securing Your Digital Assets



SIR Branch 94, February 7, 2018

<http://alanbaker.net/securing.pdf>

Alan Baker

# Credit Bureaus

- Should you be able to control who gets access to your personal financial information?

**EQUIFAX**

 Trans**Union**

 Experian

# Your Credit Bureau Rights

- Fraud Alert
  - Any new credit vendor must contact you
- Extended Fraud Alert
  - If you filed an identity theft report
  - Stops pre-screened offers
- **Credit Freeze**
  - Actually controls access to your information

**EQUIFAX**

 TransUnion

 Experian

# Credit Access Best Practices

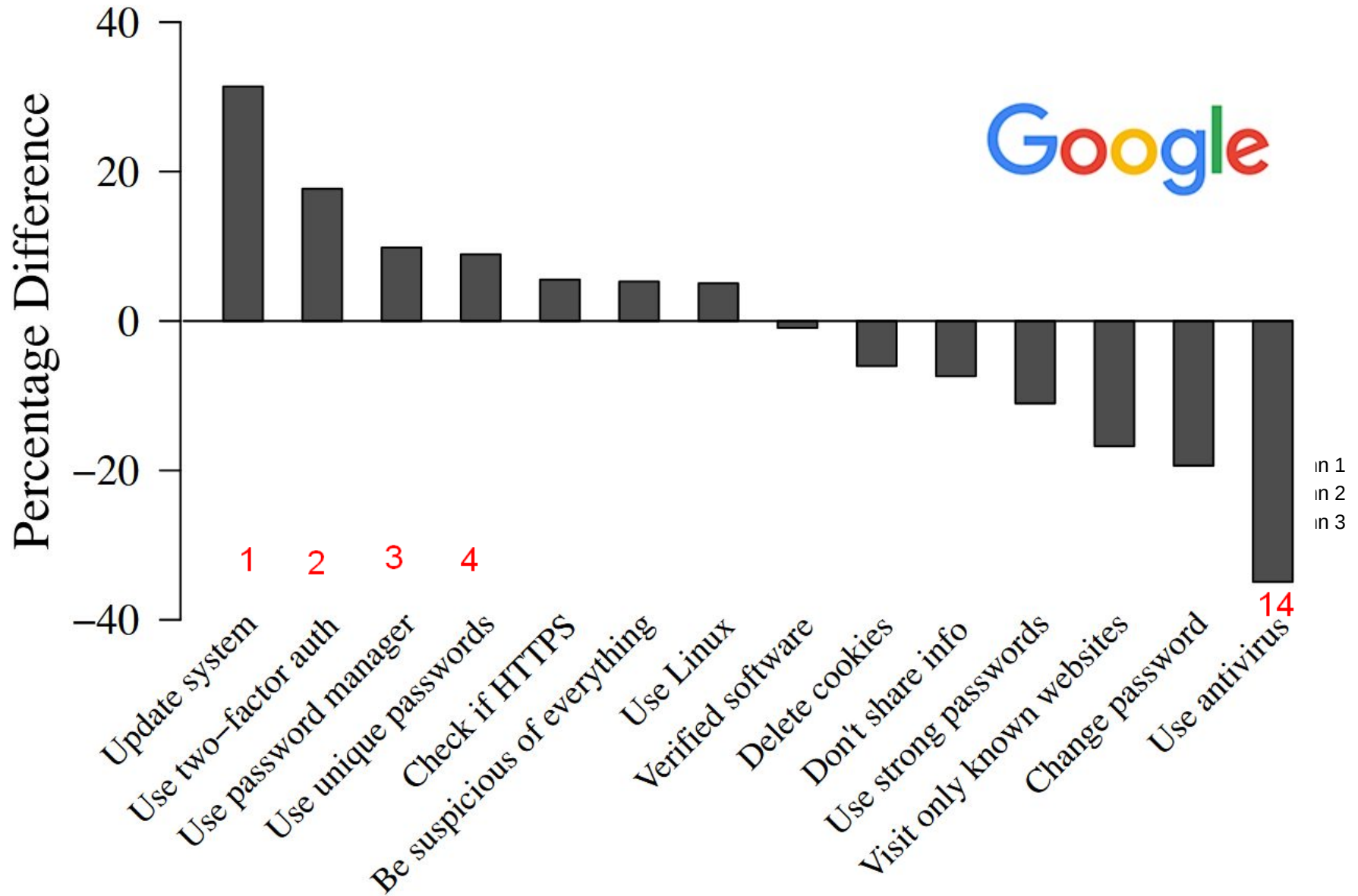
- Get **credit reports** from [annualcreditreport.com](https://annualcreditreport.com)
  - 3 times a year
- **Monitor** your bank/credit/investment accounts
- Add **two-factor authentication** to your accounts
  - Two things that you know, have, or are

**EQUIFAX**

 Trans**Union**.

 Experian

# Security Experts vs. Non-Experts



# Secure Your System



- **#1: Install all software updates**
  - **OS:** Android, Linux, iOS, Mac OS, Windows
  - **Apps:** Acrobat/Reader, Edge, Safari, Chrome, iTunes, iCloud, IE, Flash
  
- **#14: Use an antivirus program**
  - Recommended by 42% of non-experts and 7% of experts

# Secure Access to Your Accounts



- **#2 Two-factor authentication**
- **#3 Use a password manager**
  - LastPass, KeepPass, Dashlane, 1Password
- **#4 Use unique passwords**
  - Email password = bank password?

# Ransomware



**Your private key will be destroyed on:**  
**2/29/2015**

**Your personal files are encrypted!**

Your files have been safely encrypted on this PC: photos, videos, documents, etc. Click "Show encrypted files" Button to view a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a unique public key RSA-2048 generated for this computer. To decrypt files you need to obtain the **private key**.

The only copy of the private key, which will allow you to decrypt your files, is located on a secret server in the Internet; the server will eliminate the key after a time period specified in this window.

**Once this has been done, nobody will ever be able to restore files...**

**In order to decrypt the files open your personal page on site**  
**<https://34r6hq26q2h4jkzj.tor2web.fi> and follow the instruction.**

**Use your Bitcoin address to enter the site:**  
**<https://34r6hq26q2h4jkzj.onion>**

**Click to copy Bitcoin address to clipboard**

if <https://34r6hq26q2h4jkzj.tor2web.org> is not opening, please follow the steps:  
You must install this browser [www.torproject.org/projects/torbrowser.html.en](http://www.torproject.org/projects/torbrowser.html.en)  
After installation, run the browser and enter address **34r6hq26q2h4jkzj.onion**



# Avoiding Fraud and Identity Theft by Securing Your Digital Assets



SIR Branch 94, February 7, 2018

<http://alanbaker.net/securing.pdf>

Alan Baker