Personal Internet Security Basics

Agenda

- **Security is an aspiration, not a state.**
- **Encryption is your friend.**
- **Passwords are very important.**
- **Make a back-up plan.**

daniel.ficker@pantheon.io

Dan Ficker

Customer Success Engineer

dandaman on Drupal.org. deliriousguy on Twitter

Some things I enjoy, aside from coding, are

- Listening to music and live music
- Tech gadgets and the latest software
- Movies of all types

Let’s Talk Passwords

You can do passwords more securely.

Something is Wrong

- I didn’t make this change.
- Someone logged into my account!
- A phone call to Netflix confirmed that someone had changed the e-mail, the phone to some number in Peru. They just wanted to watch TV on my expense.

NETFLIX

Email changed

Hi Daniel,

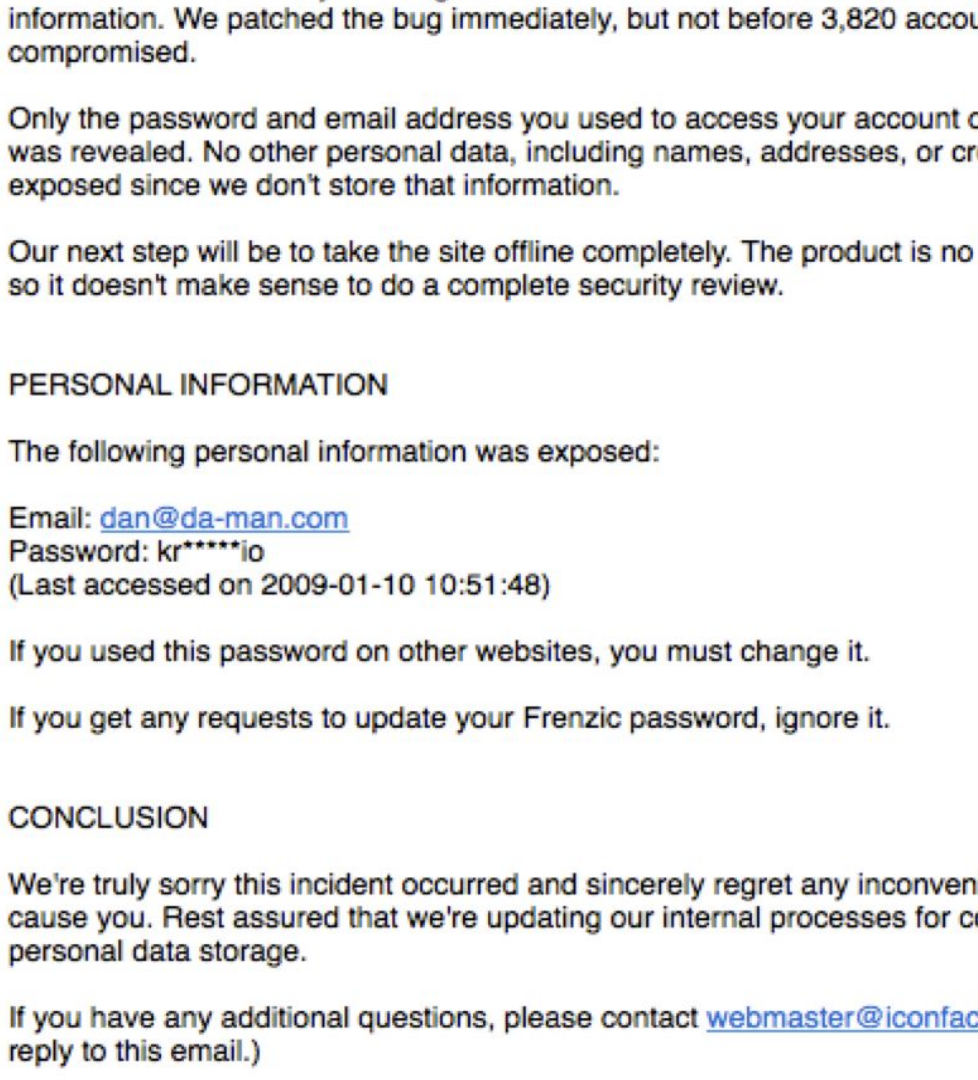
We've changed your account email address, as you asked. You will no longer be able to use [redacted]com to sign in to Netflix, please use your new email address.

If you did not ask to change your email address, we are here to help secure your account, just contact us.

–Your friends at Netflix

Earlier That Week….

- ...I got the e-mail to the right.
- In 2009, I bought a fun little game for my iPhone from a small app studio.
- I wanted to see how my score stacked up against others so I made an account on their website.
- I used my standard e-mail address and password (at the time).



information. We patched the bug immediately, but not before 3,820 accou
compromised.

Only the password and email address you used to access your account c
was revealed. No other personal data, including names, addresses, or cr
exposed since we don't store that information.

Our next step will be to take the site offline completely. The product is no
so it doesn't make sense to do a complete security review.

PERSONAL INFORMATION

The following personal information was exposed:

Email: dan@da-man.com
Password: kr*****io
(Last accessed on 2009-01-10 10:51:48)

If you used this password on other websites, you must change it.

If you get any requests to update your Frenzic password, ignore it.

CONCLUSION

We're truly sorry this incident occurred and sincerely regret any inconven
cause you. Rest assured that we're updating our internal processes for c
personal data storage.

If you have any additional questions, please contact webmaster@iconfac
reply to this email.)

Don’t Use The Same Password!

Doing so means you have to change passwords.
We all did it for a while but now it’s much too risky.

Your Password Will Not Stay Secret

What if it wasn’t Netflix but my bank, my Apple/Google account, etc?

Has Your Data Leaked?

- Visit HaveIBeenPwned.com.
- Enter your e-mail address.
- This sites aggregates data from website hacks and tells if your e-mail address and more of your account information is in available online.
- Most likely, your address and your passwords are in here.
- That means the hackers have them too.

Breaches you were pwned in

A "breach" is an incident where data has been unintentionally exposed to the public. Using the 1Password password manager helps you ensure all your passwords are strong and unique such that a breach of one service doesn't put your other services at risk.

2,844 Separate Data Breaches (unverified): In February 2018, a massive collection of almost 3,000 alleged data breaches was found online. Whilst some of the data had previously been seen in Have I Been Pwned, 2,844 of the files consisting of more than 80 million unique email addresses had not previously been seen. Each file contained both an email address and plain text password and were consequently loaded as a single "unverified" data breach.

Compromised data: Email addresses, Passwords

Adobe: In October 2013, 153 million Adobe accounts were breached with each containing an internal ID, username, email, *encrypted* password and a password hint in plain text. The password cryptography was poorly done and many were quickly resolved back to plain text. The unencrypted hints also disclosed much about the passwords adding further to the risk that hundreds of millions of Adobe customers already faced.

Compromised data: Email addresses, Password hints, Passwords, Usernames

Anti Public Combo List (unverified): In December 2016, a huge list of email address and password pairs appeared in a "combo list" referred to as "Anti Public". The list contained 458 million unique email addresses, many with multiple different passwords hacked from various online systems. The list was broadly circulated and used for "credential stuffing", that is attackers employ it in an attempt to identify other online systems where the account owner had reused their password. For detailed background on this incident, read Password reuse, credential stuffing and another billion records in Have I been pwned.

Compromised data: Email addresses, Passwords

Bitly: In May 2014, the link management company Bitly announced they'd suffered a data breach. The breach contained over 9.3 million unique email addresses, usernames and hashed passwords, most using SHA1 with a small number using bcrypt.

Compromised data: Email addresses, Passwords, Usernames

Collection #1 (unverified): In January 2019, a large collection of credential stuffing lists (combinations of email addresses and passwords used to hijack accounts on other services) was discovered being distributed on a popular hacking forum. The data contained almost 2.7 *billion* records including 773 million unique email addresses alongside passwords those addresses had used on other breached services. Full details on the incident and how to search the breached passwords are provided in the blog post The 773 Million Record "Collection #1" Data Breach.

Compromised data: Email addresses, Passwords

Dropbox: In mid-2012, Dropbox suffered a data breach which exposed the stored credentials of tens of millions of their customers. In August 2016, they forced password resets for customers they believed may be at risk. A large volume of data totalling over 68 million records was subsequently traded online and included email addresses and salted hashes of passwords (half of them SHA1, half of them bcrypt).

Better Passwords

- Should be random with alphabet, numbers, and even special characters.
- Should be long: 20-30+ characters.
- Should be unique for each site.
- No need to change passwords.
- Gov’t recommended: NIST Digital Identity Guidelines (June 2017)

Encryption

It’s math that keeps your data private.

The Internet Is Public

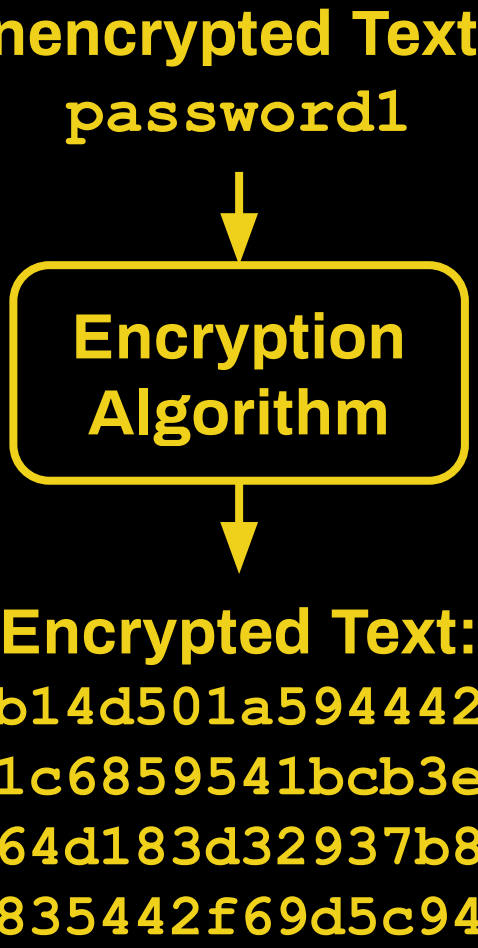
By default, all web data is sent in public
...unless we have a secret code.

Encryption is a Secret Code

Only if you know a secret can you read the code. There's a few types of encryption.

One-Way Encryption a.k.a. “Hashing”

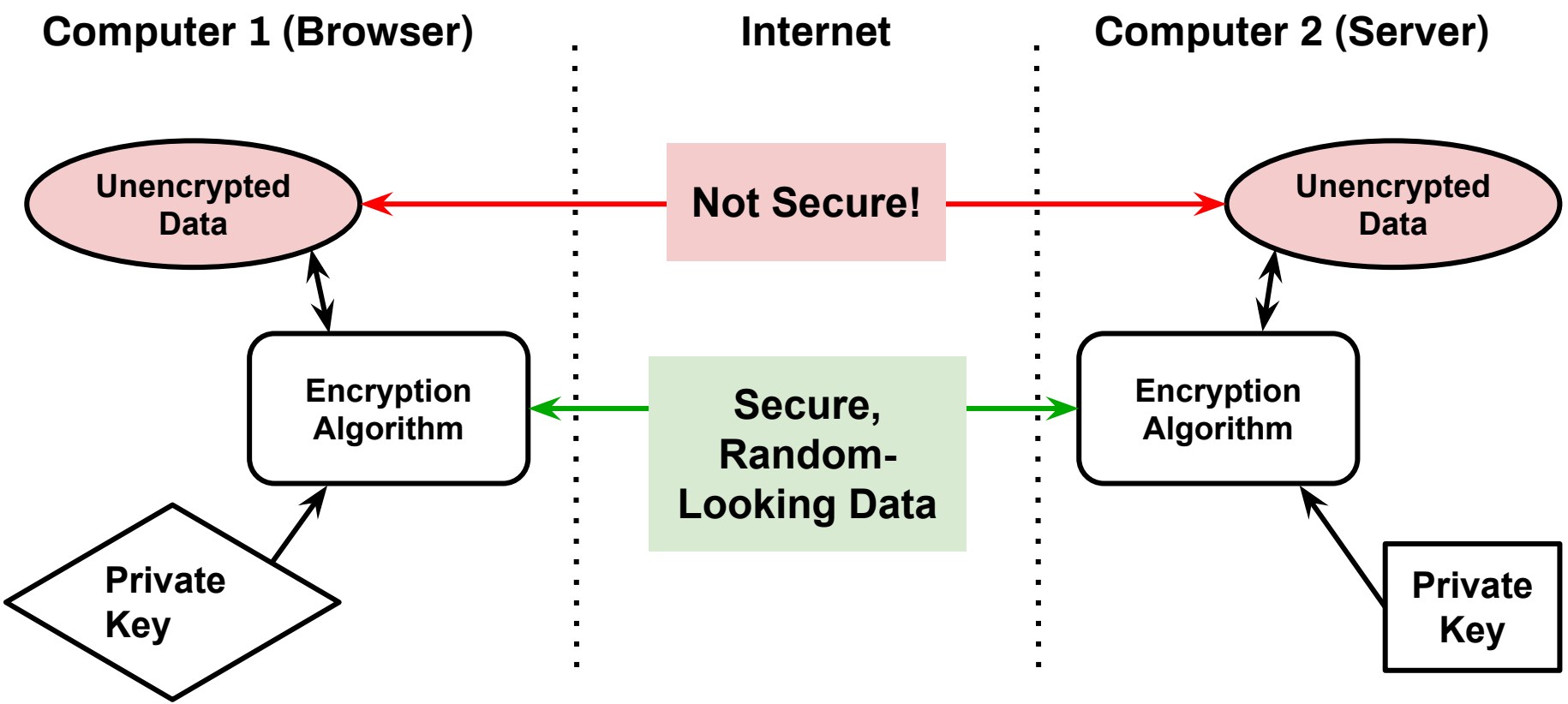
- A process of turning some text into some other text that is indecipherable from random data.
- The process is irreversible—there’s no way to get back to the original data if you only know the end result.
- This is commonly used for passwords or other data you want to use to verify but not actually keep.



Public Key Encryption

- The Private Key must be secret while the Public Key can be given freely.
- The Public Key can decrypt messages encrypted with the Private Key.
- The Public Key can encrypt messages that can only be decoded with the Private Key.
- Use Case: For storing/transmitting data that can be sensitive.

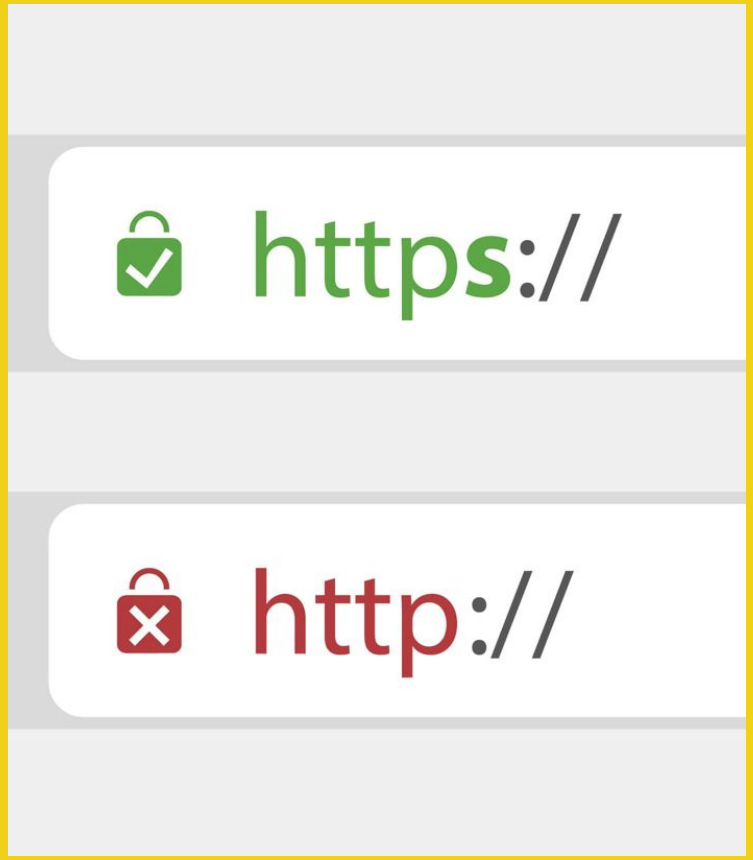
Public Key Encryption



Is Your Data Encrypted?

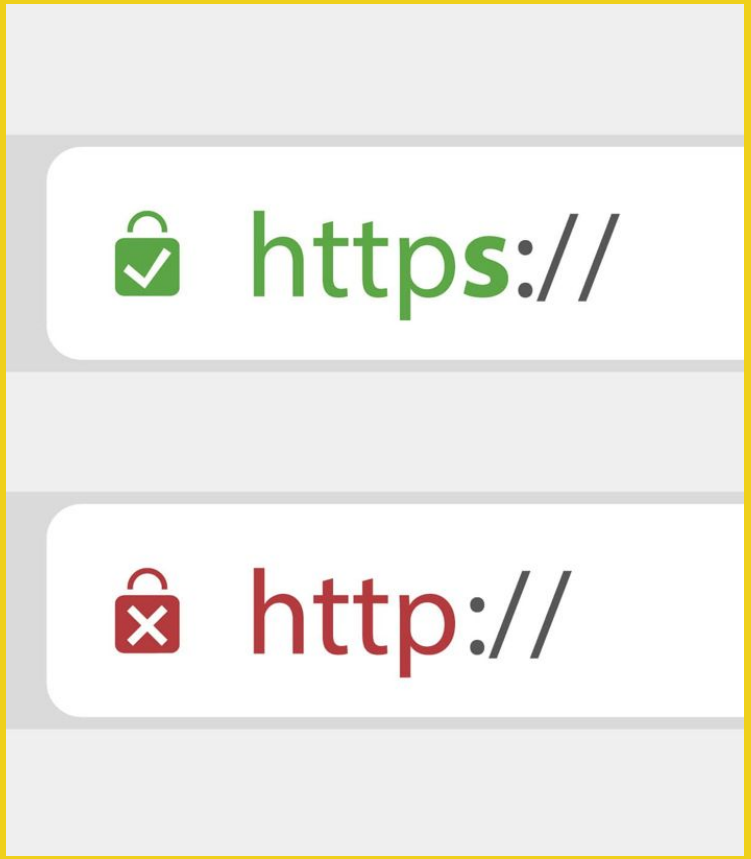
HTTPS = Encrypted

- Most major websites and apps use HTTPS. The “S” means secure.
- Encryption keeps data secret between your browser and the web server.
- Browsers often show a padlock next to the URL when HTTPS enabled.



Without HTTPS

- Anything entered on the website can be viewed/copied by any computer between you and the server. Yes, that includes passwords!
- Any router or computer between you and the server can see what page and file resources you are requesting.

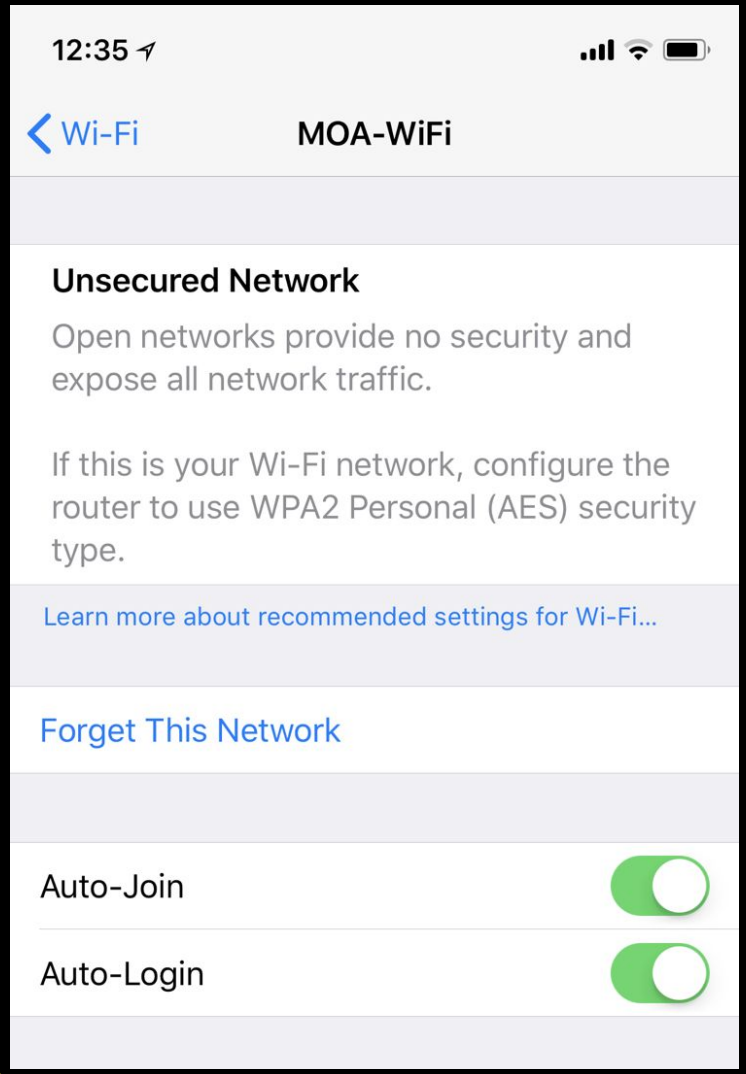


Encryption on Other Services

E-mail is not very secure, especially between providers.

FTP is not encrypted at all.

Wi-Fi can easily be insecure.



Password Managers

Your Password Vault

Log in with one password you can remember.
From there, access all your passwords.

Encrypted & Synced to Cloud

Your password decryptes. The software lets you access and fill in your passwords.

Password Managers

- **LastPass** (Free, Premium $24/year)
- **1Password** ($35/year)
- **iCloud Keychain** (Included free with Apple Devices)
- **KeePass** (Open Source)

Password Manager Features

- Plug-in integration with common browsers to auto-fill logins.
- Offers to save any login entered into the browser.
- Apps for desktop & phone OSes to access the password vault.
- Random password generator for new/updated accounts.
- Notes area for storing other data related to the account.

Multi-Factor Authentication

Types of Authentication

Authentication is the process of verifying you are who you say you are.

- Something you know.

  (e.g., password, PIN/access code)
- Something you have.

  (e.g., card, fob, token)
- Something you are.

  (e.g., fingerprint, face, DNA)

Uses of Other Factors

Temporary Factor Replacement

- Quicker way to login
- Falls back to more secure factor
- Some factors are not good legally
- Example: iPhone allows Touch ID/Face ID instead of Password

Two-Factor Autentication

- **Both are Required for Access**
- **More secure**
- **Even if someone gets your password (“know”), they also need a key fob or token (“have”) so it’s somewhat useless without it.**

Security, Continued

Some miscellaneous items

Phone Number Verification

Problem: Phone numbers can be insecure.

- Customer Service people may do the wrong thing when coerced.
- The backend phone network is mostly insecure. Bad actors may be able to add themselves to your account.

Solution: Don’t do verification via SMS. Do it via an app on your phone.

- **Google, Twitter, Facebook, etc. all offer this option.**
- **Note: Need to remember to deal with this when changing phones.**

Password Recovery

Problem: If your passwords are good, the weak spot is the company's policy for recovering your password.

- Bad actors may be able to figure out your mother's maiden name, your birth date, your city of birth, maybe even your first pet.

Solution: Create some random words (that can be said to customer service over phone, if needed) that have nothing to do with the question.

- **Store the question and your answer in password manager "notes" area.**

Trust vs. Security

Who do you trust to keep your data safe?

You don’t have to trust a provider if you encrypt the data before transmitting or storing.

To some extent, you have to trust:

- **Your Internet Service Providers**
- **Your Phone Company**
- **Your Cloud Service Providers**

Trust No One

- Systems can be built so that you hold all the keys—the providers can’t look at your data even if they want to without your password.
- For example, if you lose your 1Password or LastPass login/password, they really can never get that data back for you.

- **You control your destiny and security.**
- **With great power comes great responsibility. Keep the keys safe!**

BACK UP!

- Have an automated back up plan for important data.
- Back up data on-site as well as off-site.
- For really important data, maybe even put it in a safe deposit box or something.

Any Questions?

Slides:
2019.drupalcorn.org/session/personal-internet-security-basics

Thanks for coming!

Steve Gibson

- Security Researcher, Developer
- New idea for a slick, password-less login system, SQRL
- Gibson Research Corp: GRC.com

Host of Security Now! Podcast

- **700+ in-depth episodes spanning 13+ yrs**
- **Much presented in session learned here**