Personal Internet Security Basics

Dan Ficker

Twin Cities DrupalCamp 2018

Overview

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

About Me

- Computer geek since age 11
- PHP Developer for 13 years
- Drupal Developer for 8+ years
- Blog: http://da-Man.com/
- Twitter: @deliriousguy
- Currently employed by

AUGUST ASH

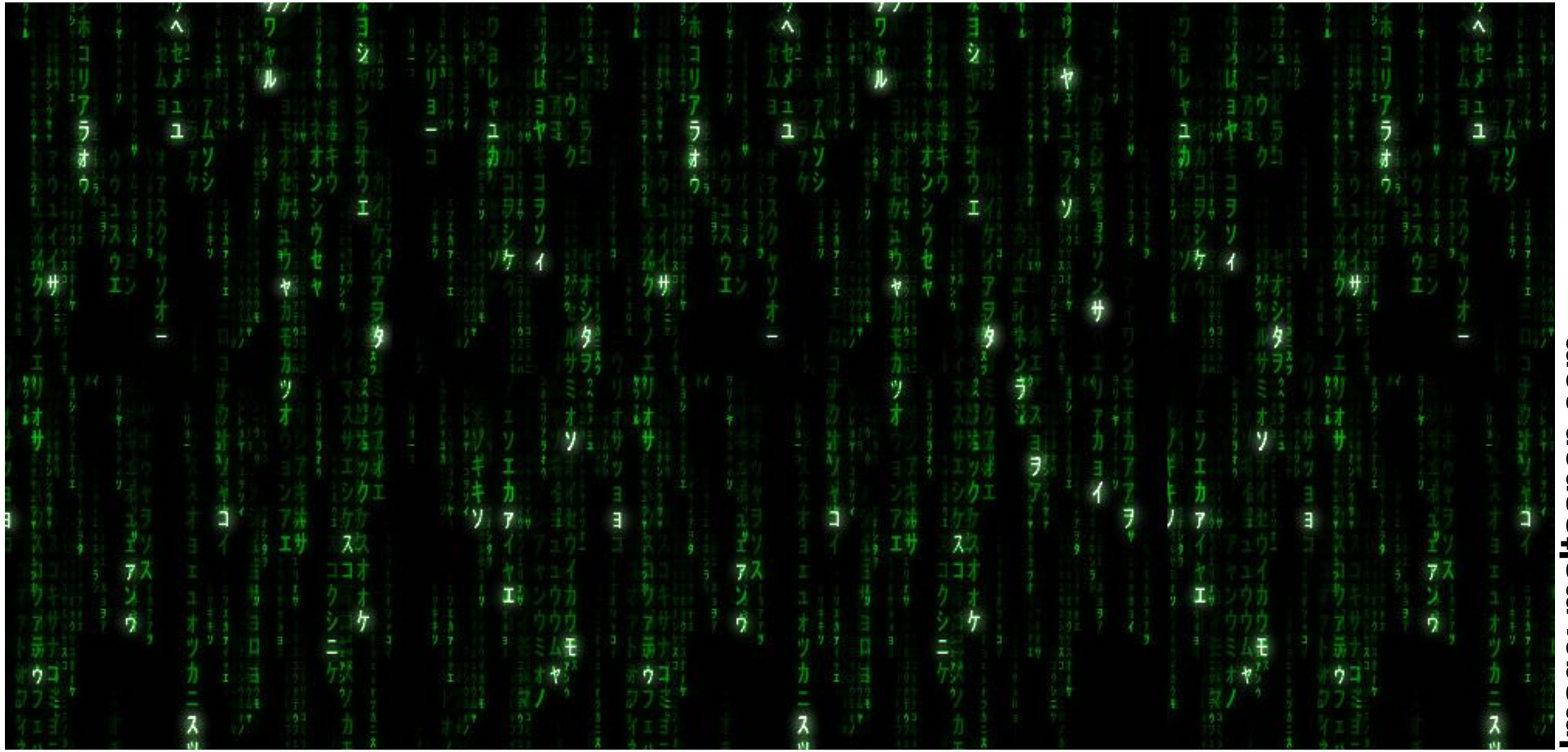


Image: maltaanon.com

Let’s Talk Encryption

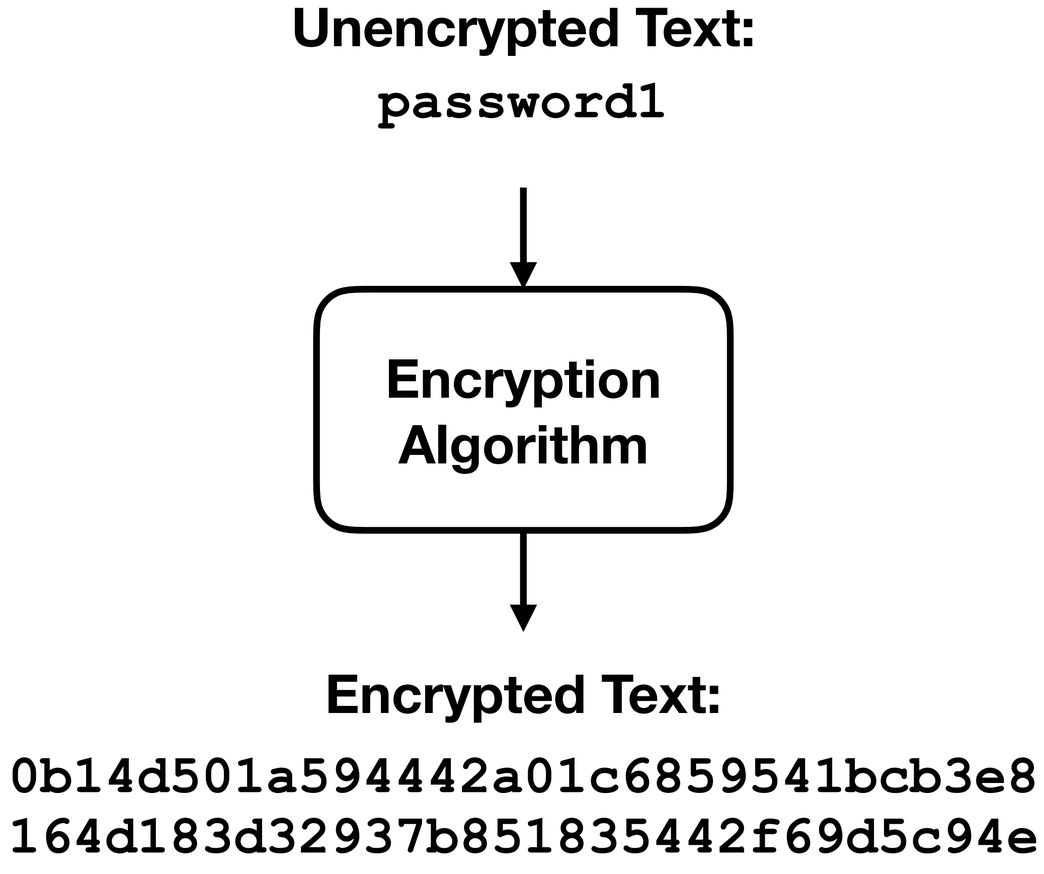
Math That Keeps Your Data Private

Why Encryption?

- The Internet is a series of data packets passed between computers.
- Much like the mail, many computers (and their owners) are sent this data and pass it along.
- Without encryption, they could open the data and read your correspondence.
- Encryption acts like a secret code between the sender and receiver.

One-Way Encryption

- Also known as “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.
- Public Key can decrypt messages encrypted with the Private Key.
- Public Key can encrypt messages that can only be decoded with the Private Key.
- Great for storing/transmitting data that can be sensitive.

Public Key Encryption

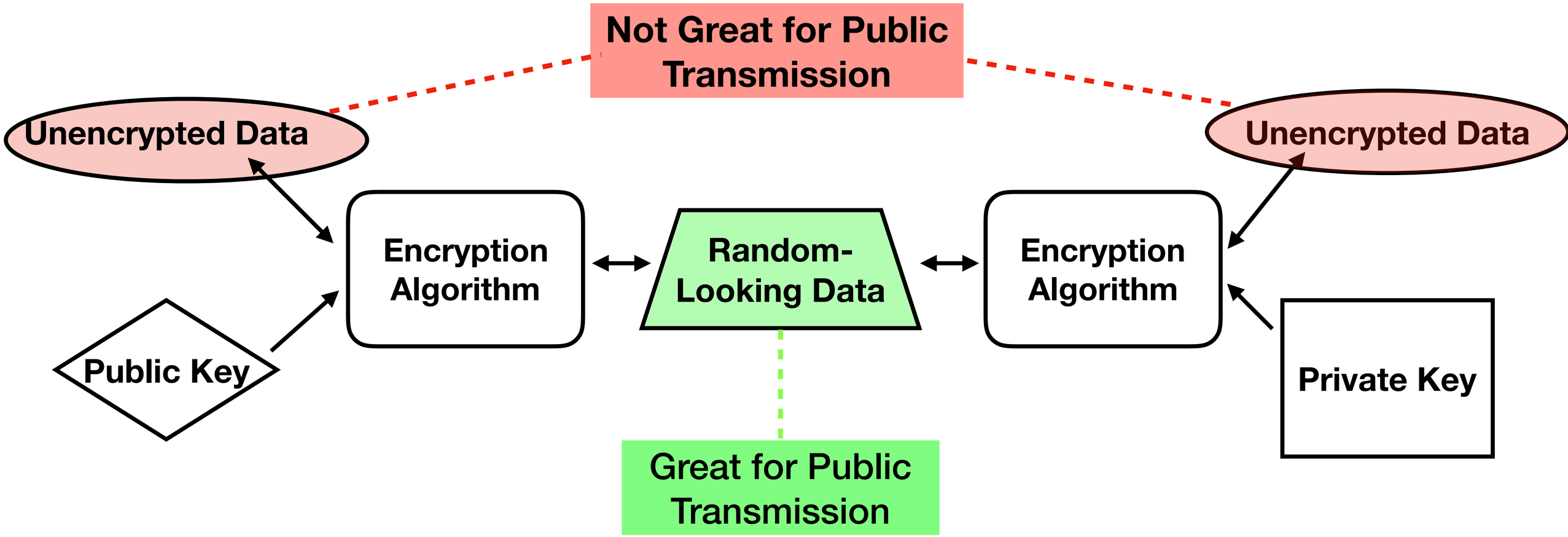


Image: Universal Pictures

When Is 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.

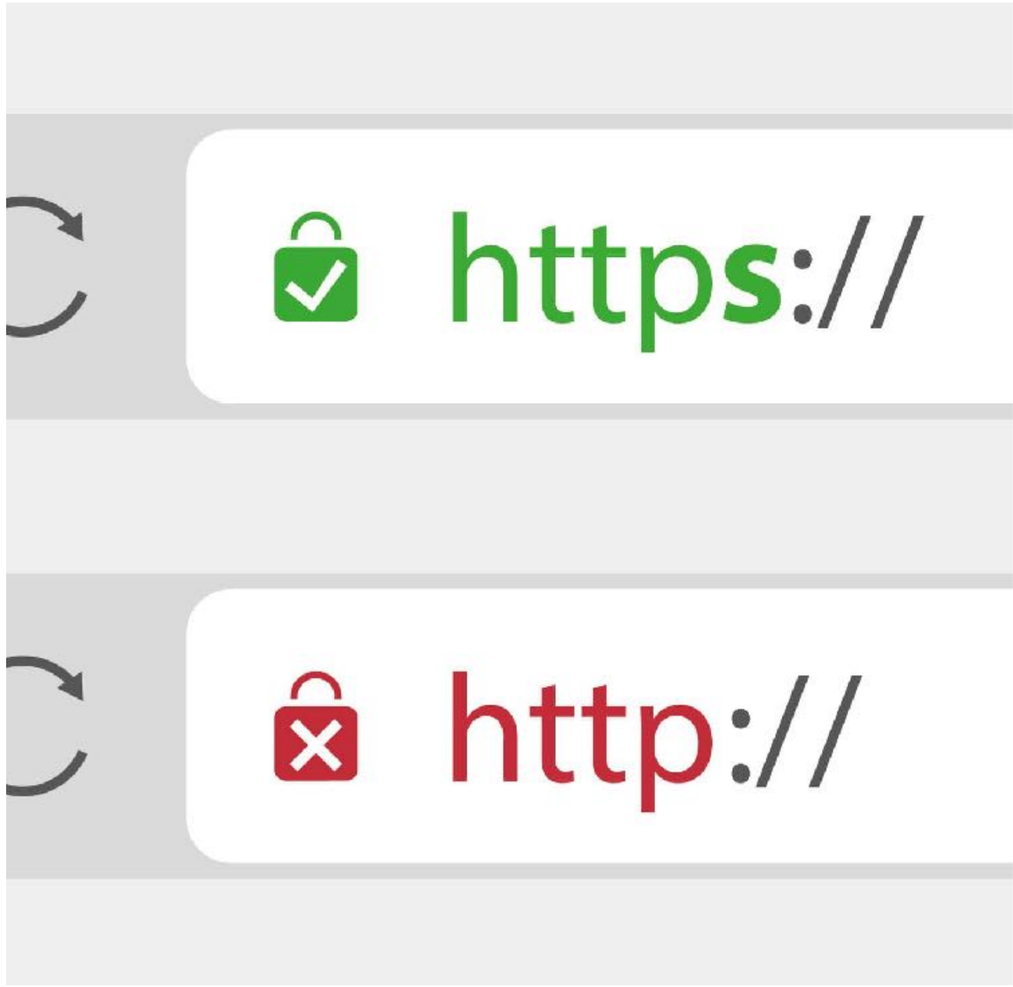


Image: Animaweb

HTTPS (Continued)

- Without HTTPS, anything entered on the website can be viewed/copied by any computer between you and the server. Yes, that includes passwords!
- Without HTTPS, any router or computer between you and the server can see what page and file resources you are requesting. With HTTPS, they only can see what server you are requesting data from.
- E-mail can be sent to & from e-mail servers in an encrypted manner using TLS, but there's no real guarantees that this will happen. **E-mail should be considered insecure.**
- At this point, just because HTTPS is not used does not mean someone will see your data. But it is a risk you take if not encrypting communications.

Wi-Fi

- Wireless Internet means you're publicly sending data over radio waves between you and the access point.
- Anyone who can pick up that radio signal may be able to get some info about you.
- Only Wi-Fi Networks that require a password and use WPA encryption create a secure tunnel between your computer and the access point.

Image: Information Age

Let’s Talk Passwords

Verifying your digital identity since 1961

Passwords (Traditional)

- Come up with one or a few passwords that you can remember.
- Use them for everything.
- Add on a number or symbol at the end. Change it occasionally.
- Forget the password and then have to go through a reset process.

Password Problems

- It used to be you had passwords for a few work things and the bank account, but now we used hundreds of sites, each with a password.
- Some of these sites get hacked and the passwords get out.
- Now you should probably change that same password on every site.
- You only have one/few passwords because they’re hard to remember.

Passwords Get Loose

- 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.
- They did not use one-way encryption; they just stored my password unencrypted.
- In February, I got the e-mail to the right. My e-mail address and password was out.

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

Our next step will be to take the site offline completely. The product is
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.

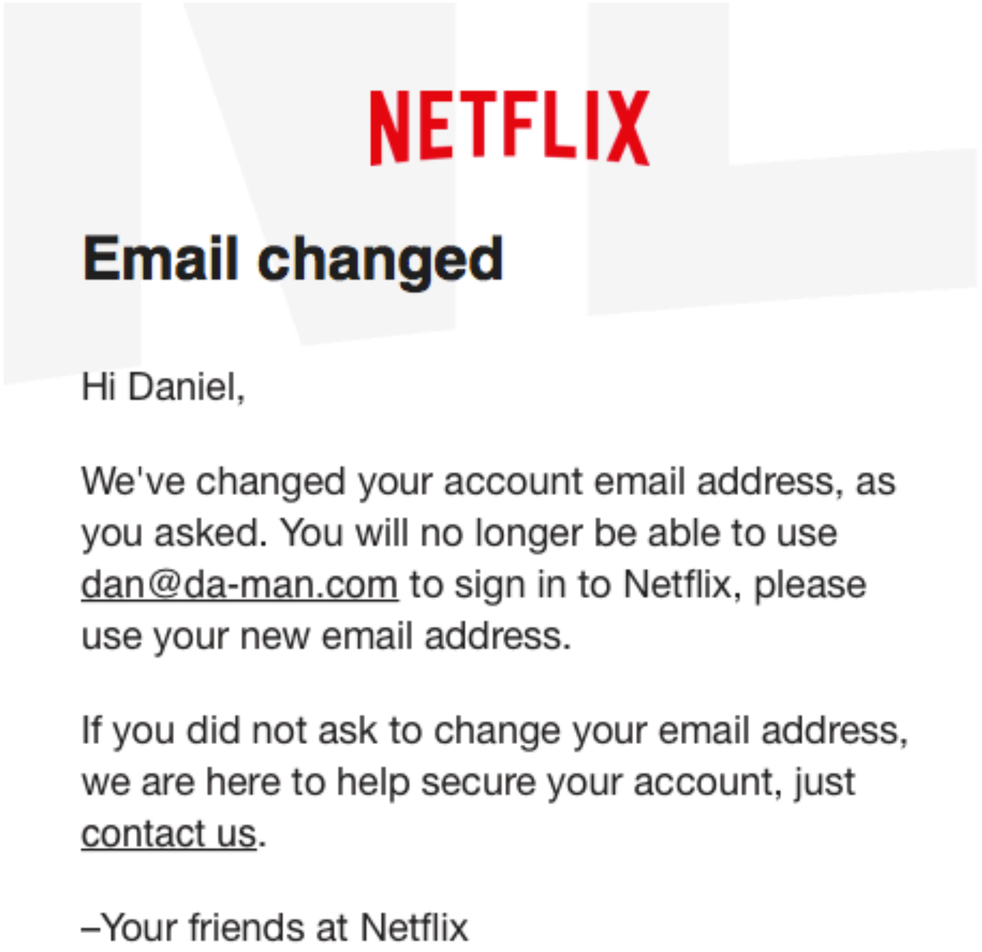
If you get any requests to update your Frenzic password, ignore it.

CONCLUSION

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

Passwords Loose!

- Two days later, I get an e-mail from Netflix that notified me that someone logged into my account and changed the e-mail address.
- I didn’t do that and—oh crap!—I used that same password that was recently disclosed.
- 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 dan@da-man.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.

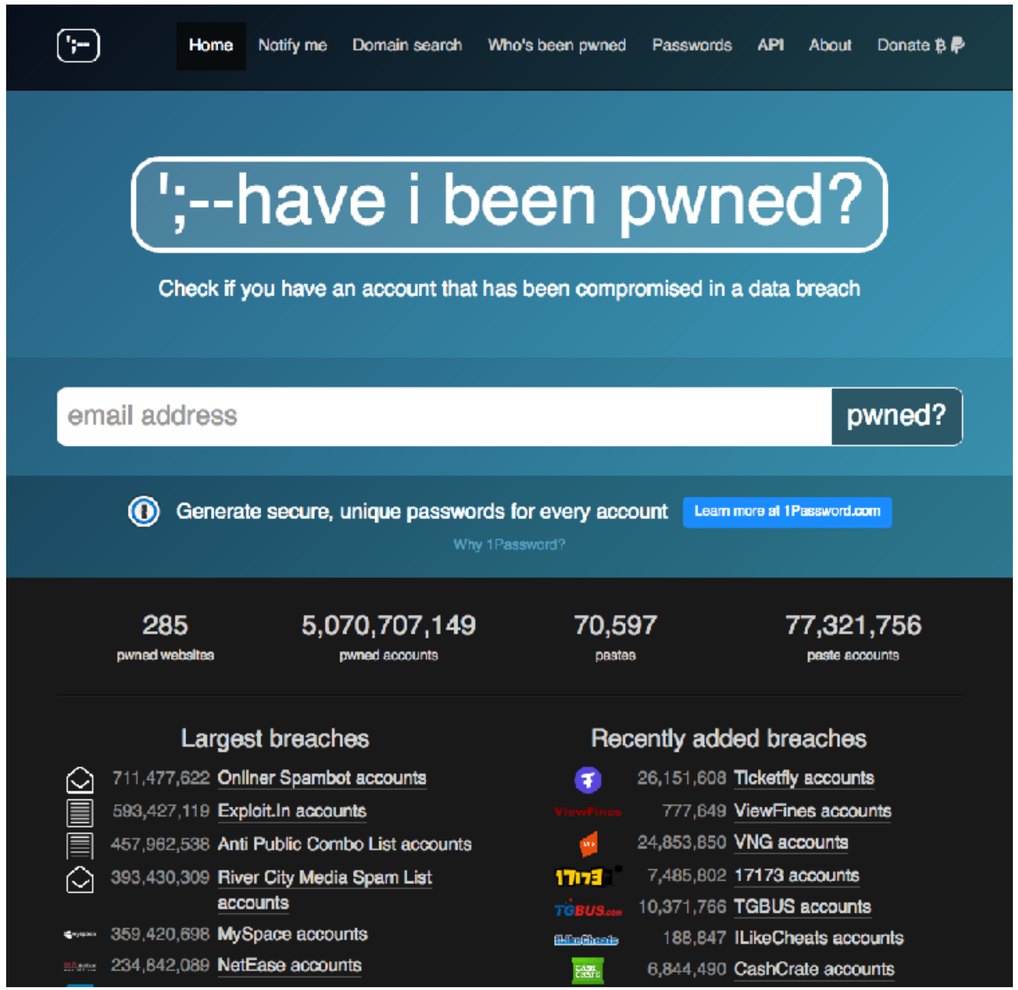
–Your friends at Netflix

What We Learned

- You give your password to the company that manages that account. They might not even encrypt that password correctly.
- The company may give this password to others, intentionally or unintentionally. If used in many places, this can be a problem.
- Hacking my Netflix account, they can’t get much useful info about me, just hope I pay for their binges for a bit. So not a huge security risk.
- But what if it was my bank? My e-mail? My Apple/Amazon account?

Has Your Data Leaked?

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



Better Passwords

- Should be random with alphabet, numbers, and even special characters.
- Should be long: 20-30+ characters long. The more the better.
- Should be unique for each site or service.
- No need to change password regularly with above recommendations.
- Government recommended: NIST Digital Identity Guidelines (June 2017)

Password Managers

- These passwords are impossible to remember. That’s a **good thing**.
- A “Password Manager” is an encrypted vault of all your passwords.
- You need to remember just one password to get into your vault.
- Optionally, use multiple factors as well to protect this vault of data.

Password Managers

- The best available:
  - LastPass (Free service, 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

Security on top of Security

Factor Types

- Authentication is the process of verifying you are the account holder.
- Three factors of authentication:
  - 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)

Multiple Factors

- Sometimes, one of the factors is used as a quicker, temporary way to login.
  - For example, iPhones allow for fingerprint/face recognition instead of passwords for some operations.
  - Legally, something you have or are may be easier for enemies to get than something you know.
- Even better, require two factors for better security.
  - Even if someone gets your password (“know”), they also need a key fob or token (“have”) so it’s somewhat useless without it.

Two-Step Verification

- Some secondary verification is still something you know.
- It’s not something you have or are, but some other message you should be able to know if you are who is expected.
- This includes getting a code on another device then entering it when prompted.
- Not multiple factors, but two-step verification can still be more secure.

COMEDY 09/11/2009 05:12 am ET | **Updated** Dec 06, 2017

Google Lets Privacy Critics Opt-Out, Relocate To Remote Village (VIDEO)

Are you tired of Google knowing your every move, every thought, want, purchase, opinion? Then Google's new opt-out village is for you...as long as you know how to farm and bury a dead body.

WATCH:

Other Security Considerations

Phone Number Verification

- **Problem:** Phone Numbers can be somewhat 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.
    - Your mother's maiden name, your birth date, your city of birth, maybe even your first pet are things that bad actors may be able to figure out.
- **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?
- To some extent, you have to trust:
  - Your Internet Service Providers
  - Your Phone Company
  - Your Cloud Service Providers (if any)
- Beyond that, make sure encryption of data is happening.

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 LastPast login/password, they really can never get that data back for you.
- This means you control your destiny and security.
- **With great power comes great responsibility. Keep the keys safe!**

Back Up!

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

Thank You!

Any Questions?

The Steve Gibson Slide

- Host of Security Now! Podcast
  - 650+ in-depth episodes spanning 13 yrs
  - Much presented in session learned here
- Security Researcher, Developer
- New idea for a slick, password-less login system, SQRL
- Gibson Research Corp: GRC.com