

Basic Cyber Security

2018 NCAVA Annual Conference

Blake Irwin

whoami

- Blake Irwin
 - Senior Cyber Security Analyst
 - 10 years IT and Cyber Security experience
 - Help Desk
 - Systems/Network Administrator
 - Incident Responder, Cyber Defender, Security Tester, Security Engineer
 - Worked in education, financial, healthcare, manufacturing industries
 - Certifications:
 - CISSP, GPEN, GWAPT, Nexpose Certified Administrator, Security+

Security is a journey not a destination

Overview

- Threats
- Account Security
- Device Security

Threats

Definitions

- Asset – what we try to protect
 - Threat – what we try to protect against
 - Vulnerability – a weakness or gap
 - Risk – impact to an asset due to a threat exploiting a vulnerability
-
- A little math
 - $\text{Asset} + \text{Threat} + \text{Vulnerability} = \text{Risk}$

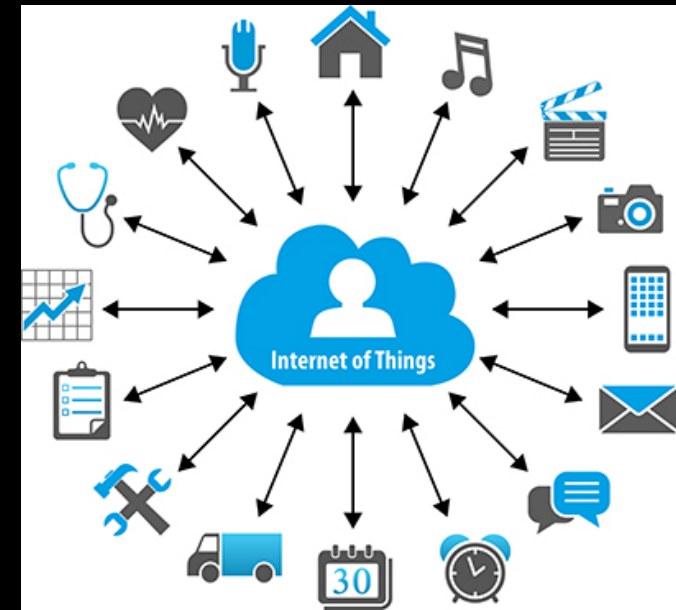
What is YOUR Risk Profile?

- What do YOU want to protect?
 - What threats are YOU protecting against?
 - Do YOU have any known weaknesses?
-
- What is YOUR risk profile?

Emerging Threats

Emerging Threats

- Phishing
- Internet of (Insecure) Things
- Ransomware



Everyday Threats

Everyday Threats

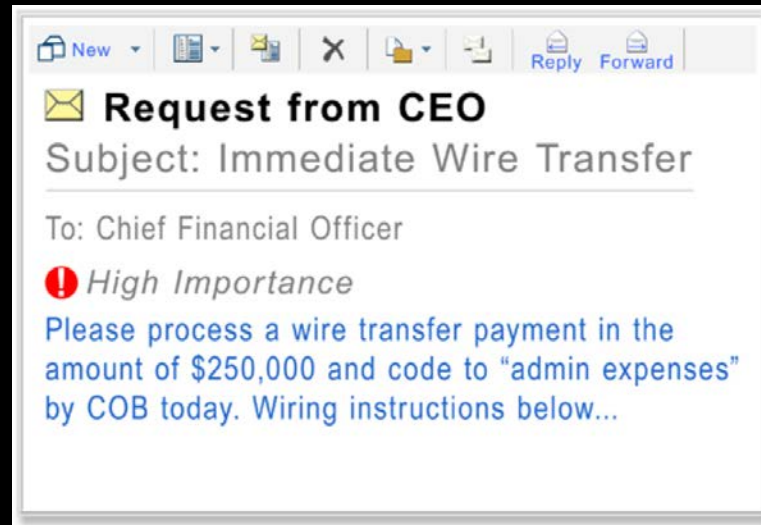
- Phishing
- Account Compromise
- Scams
- Malware
- Social Engineering
- Lost/Stolen Device
- Accidental/Unintentional disclosure
- Vendor Trust
- The Dark Web


What is Phishing?

- Sending fraudulent emails in order to trick the recipient into taking an action resulting in disclosure of personal information, clicking of a link, or taking an out-of-band action.

Types of Phishing

- Spam
- Phishing
- Whaling
- CEO Fraud
 - Corporate
 - Personal
 - The Little Family




STATON LAW FMBC CORPORATION
210 Third Avenue West
Hendersonville, NC 28739

Wiring Instructions:

Name of Bank:	Bank Of America
Bank Address:	6 Tremont street, Boston MA 02108
ABA Number:	026009593
Beneficiary:	STATON LAW FMBC CORPORATION
Account Number:	[REDACTED]

****The wire transfer must have buyer/borrower name on it please.**

Why does phishing work?

- Attackers exploit human nature
- Play on emotions
 - Fear, Urgency, Trust, Luck
- Context
- Trust

Signs of a phish

- Sender, normal address?
- Look a like domain?
- When was email sent?
- Was I expecting this?
- Did email create emotional response?
 - Upset, too good to be true, fear
- Is email trying to make me take action?
- Are details to general, wrong, odd, or illogical?
- Do links go where they say they go?

Phishing Examples



Example 1

- Email with .HTML attachment
- Link in attachment
- Takes you to fake payment page

From: **Squarespace Support** <wordpress@sekjdiir.wpengine.com>
Date: Thu, Feb 1, 2018 at 4:09 AM
Subject: Credit Card Payment Due
To: [REDACTED]

Dear [REDACTED] This is a notice to remind you that you have an invoice due on 02/01/2018. We tried to bill you automatically but were unable to because we don't have your credit card details on file. Invoice Date: 02/01/2018 Invoice #5155681 Amount Due: \$59.90 USD Due Date: 02/01/2018 Attached is a copy of your most recent transaction.

Please Verify Your Card Information

Status of Payment. If a credit card is present on your account we have attempted to charge that payment method for balances due.

There was an error renewing your connected domain due to incorrect billings provided

We tried to bill you automatically but were unable to because we don't have your credit card details on file.

Please login to our client area at the link below to submit your card details or make payment using a different method.

[Use Payment](#)

After numerous attempts to process your payment, we were unable to renew your connect domain
This means:

Your features will be canceled
Your domain name will be disconnected from your website

To keep your domains active and prevent service interruptions:

- Check that auto-renew is enabled in the Billing panel.
- Check that your billing credit card is up to date

Example 2

- Strange extortion ransom

From: nicole.ramsey1970@zipmail.com.br <nicole.ramsey1970@zipmail.com.br>
Sent: Friday, May 4, 2018 12:15 AM
To: [REDACTED]
Subject: [REDACTED] Be smarter next time ID eyjt035

[REDACTED]

Your PC was attacked by the corruptive application .

Whats the scam?

I deposited my malicious agent on a hard-core online portal, you pressed this information and urgently installed the malicious software to your system .

That rogue program made your front camera making video in such a way I get a clip with you dash your doodle.

During the next 5 hours this rogue program hijacked all the contact numbers numbers.

At this moment, I got all your information and movie with you burp the worm, now in a case if you wish me to eliminate all the contact information forward me 376 U.S. dollars in BTC digital currency.

In other circumstances I would forward the videotape to all your contacts .

I provide you mine Bitcoin wallet - 18dAWrPkVGEAFDSHs68C9gnnqhD4prggxW You get 24 hours after getting this. If I obtain transaction I am going to annul the videotape for ever and aye.

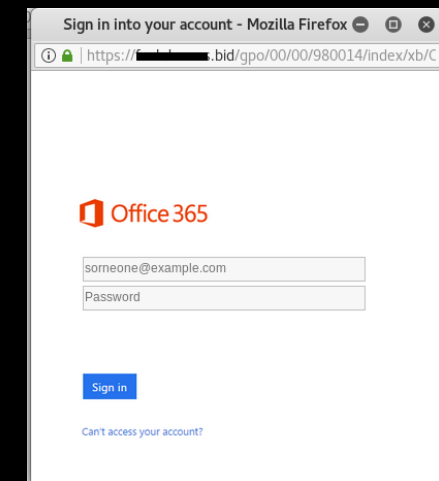
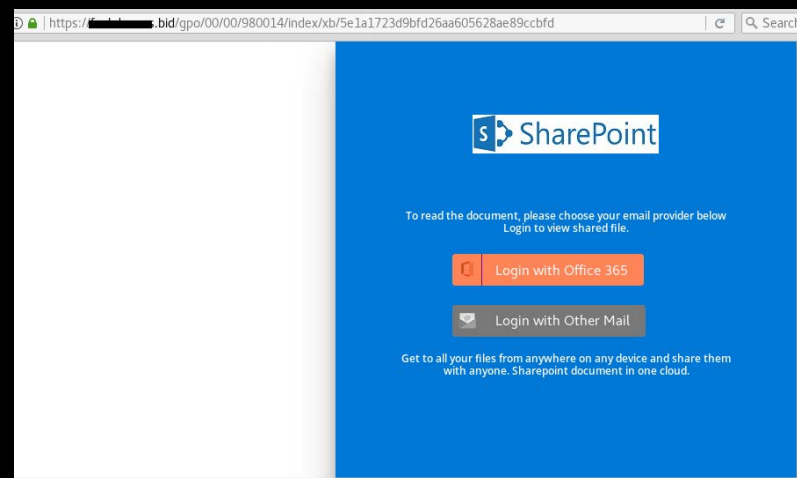
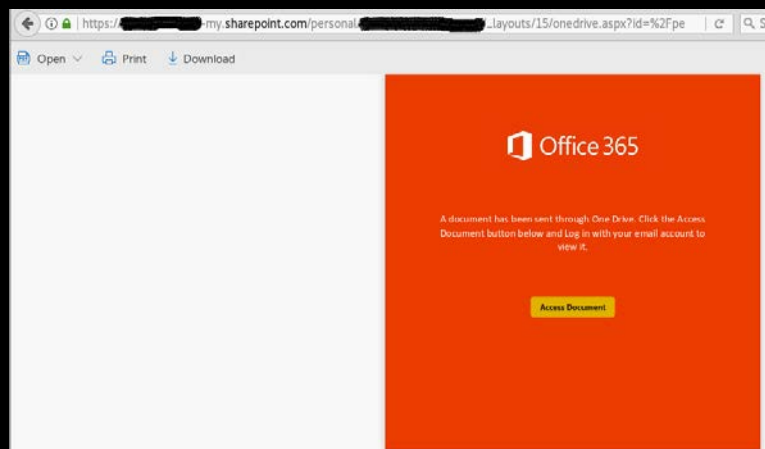
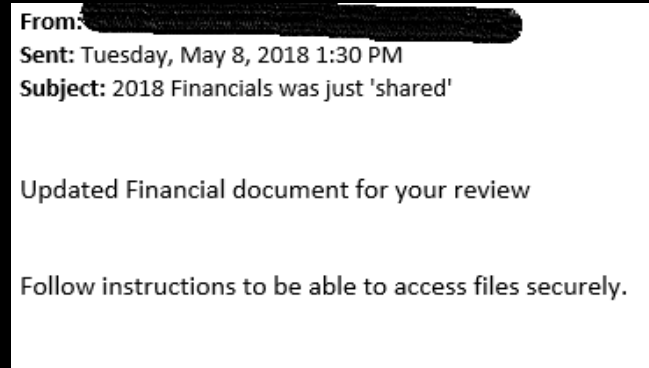
Im sorry for m y mistakes- I'm Chineeze .

P.S. this mail address, I have plundered hobbled it.

Don't reply to this email. This is temporary email address!

Example 3

- Credential Stealing Phish
- Compromised Email
- Advanced Attack



Account Compromise

- Unauthorized access to an account.
- Generally occurs through valid credentials.

How was my account compromised?

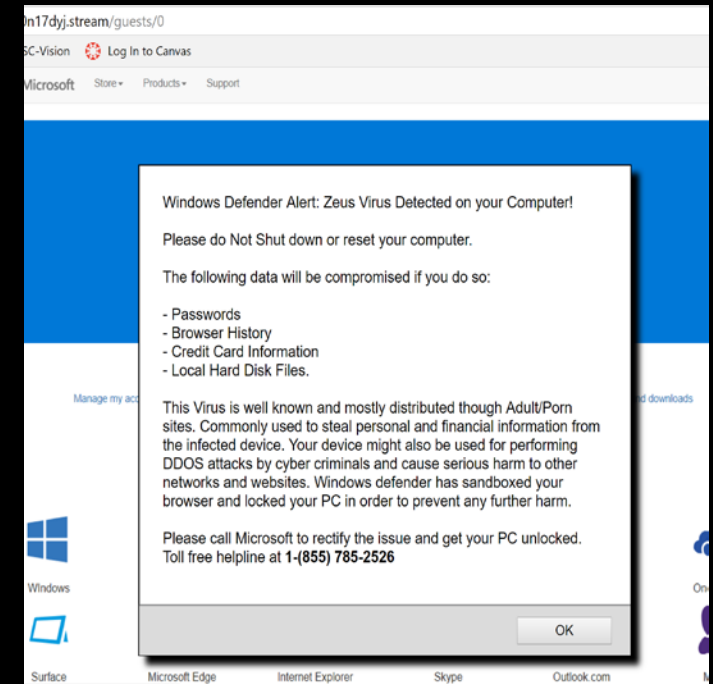
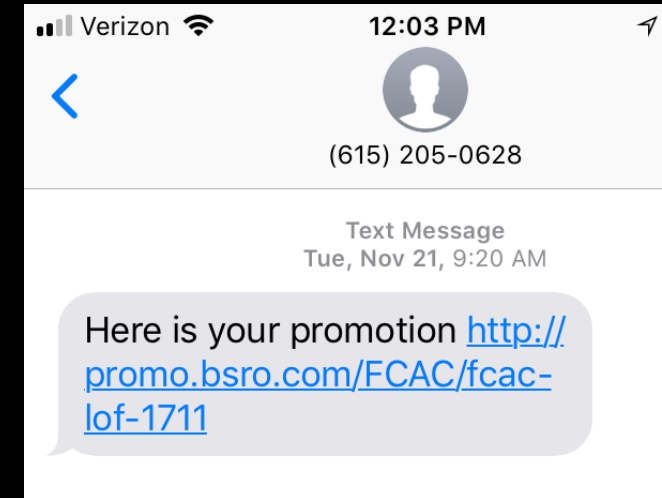
- Stolen Credentials
- Password Guessing
- Malware
- Social Engineering
- Password Reuse

Why are accounts compromised?

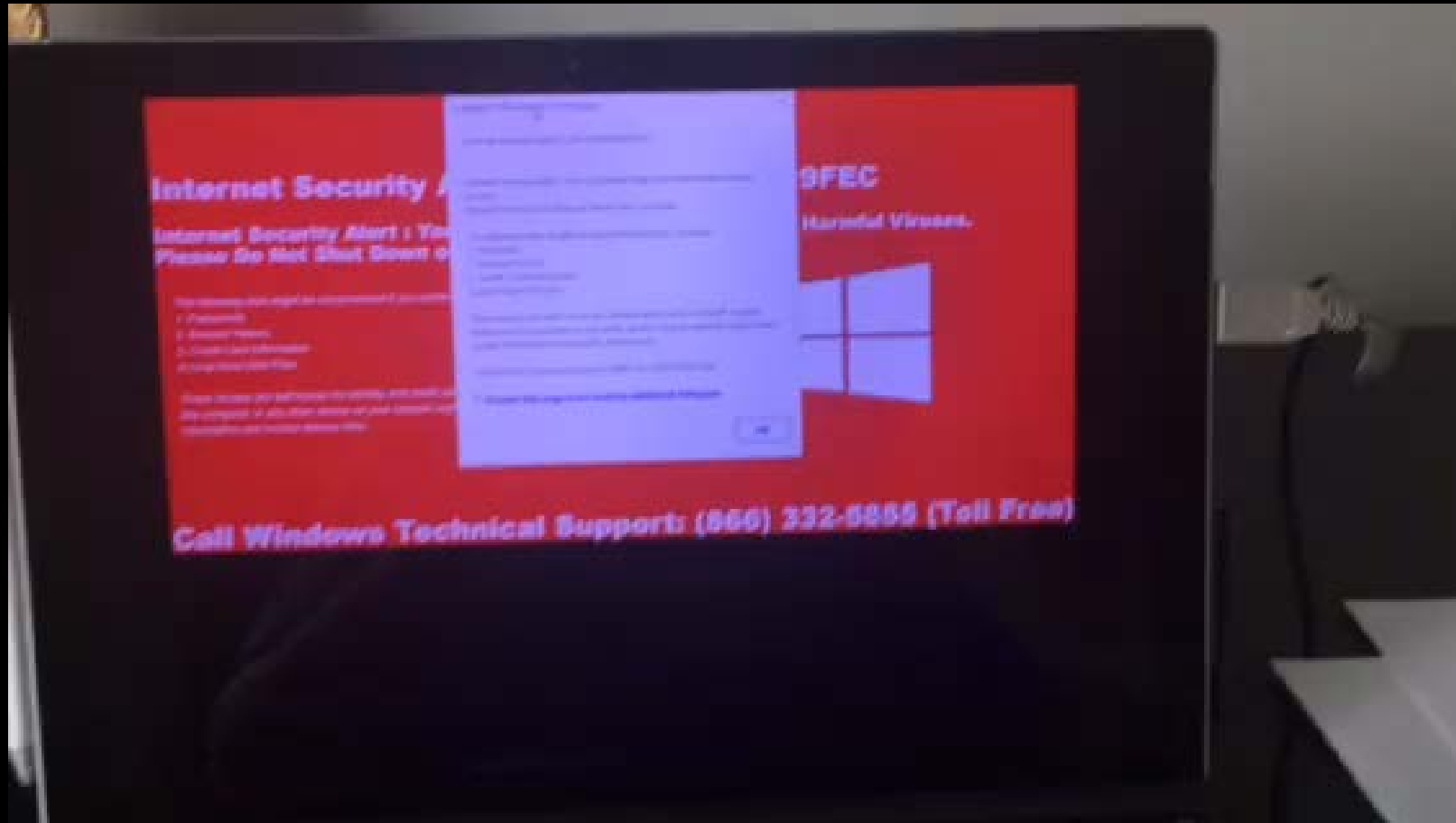
- Spam/phishing
- Steal personal information
- Fraud
- Reputation damage (social media)
- Data destruction
- Extortion
- Sell on black market
- **Most roads lead to Financial Gain**

Scams

- Vishing
 - Telephone equivalent of phishing
- SMiShing
 - Text message (SMS) equivalent of phishing
- Scareware
 - Web browser pop-up or redirect to “scary” site



Scareware



Malware

- Malicious software
 - Bundled with legitimate software
 - Silently installed from “bad” website
- Examples of malware
 - Ransomware
 - Keylogger
 - Botnet
 - Worm
 - WannaCry was a ransomware worm.

Other Threats

- Social Engineering
- Lost/Stolen Device
- Accidental/Unintentional disclosure
- Vendor Trust
- The Dark Web

So I fell for the trap, now what?



I was phished, now what?

- Do not reply to the phishing email
- Report email as phishing
 - Report to webmail vendor or work as fraud
 - If personal, report to IC3.gov
- Contact your IT support if clicked.
- If credentials were entered, change password immediately
 - From clean device
- Delete the email when appropriate

My password was stolen

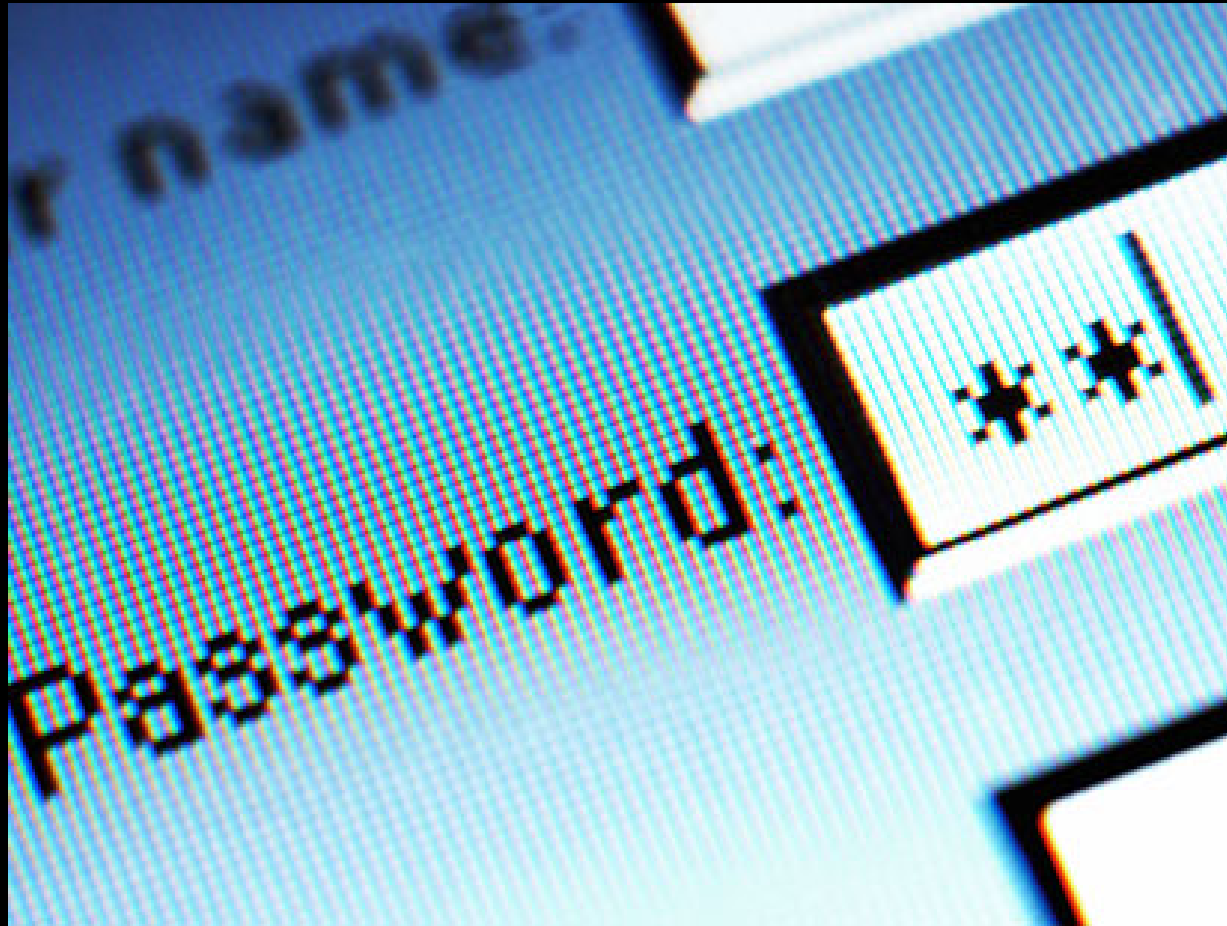
- Change password from a clean machine
- Turn on multi-factor authentication (if available)
- Review account for any changes

My device was lost/stolen

- If tracking enabled, try Find My iPhone (or similar technology)
- If not found, initiate remote wipe (if possible)
- Hope for the best...
- If sensitive data was on the device, use encryption going forward

Account Security

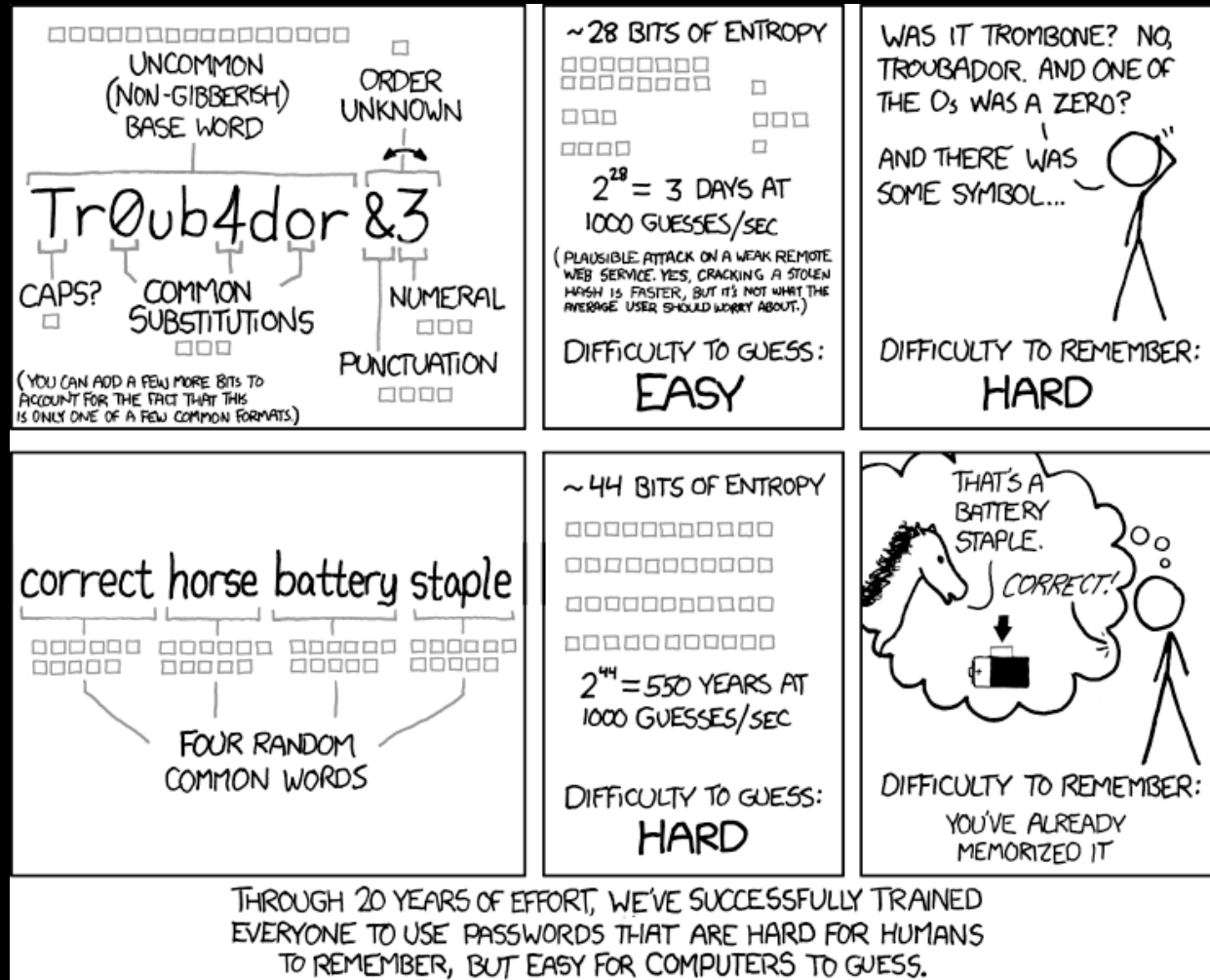
Passwords



Password Best Practices

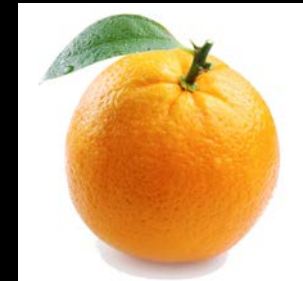
- Never re-use passwords
- Use long passwords (12+ characters)
- Use complex passwords
- Use a passphrase
- Change password periodically

Password Strength Visualized



The Blake Password Method

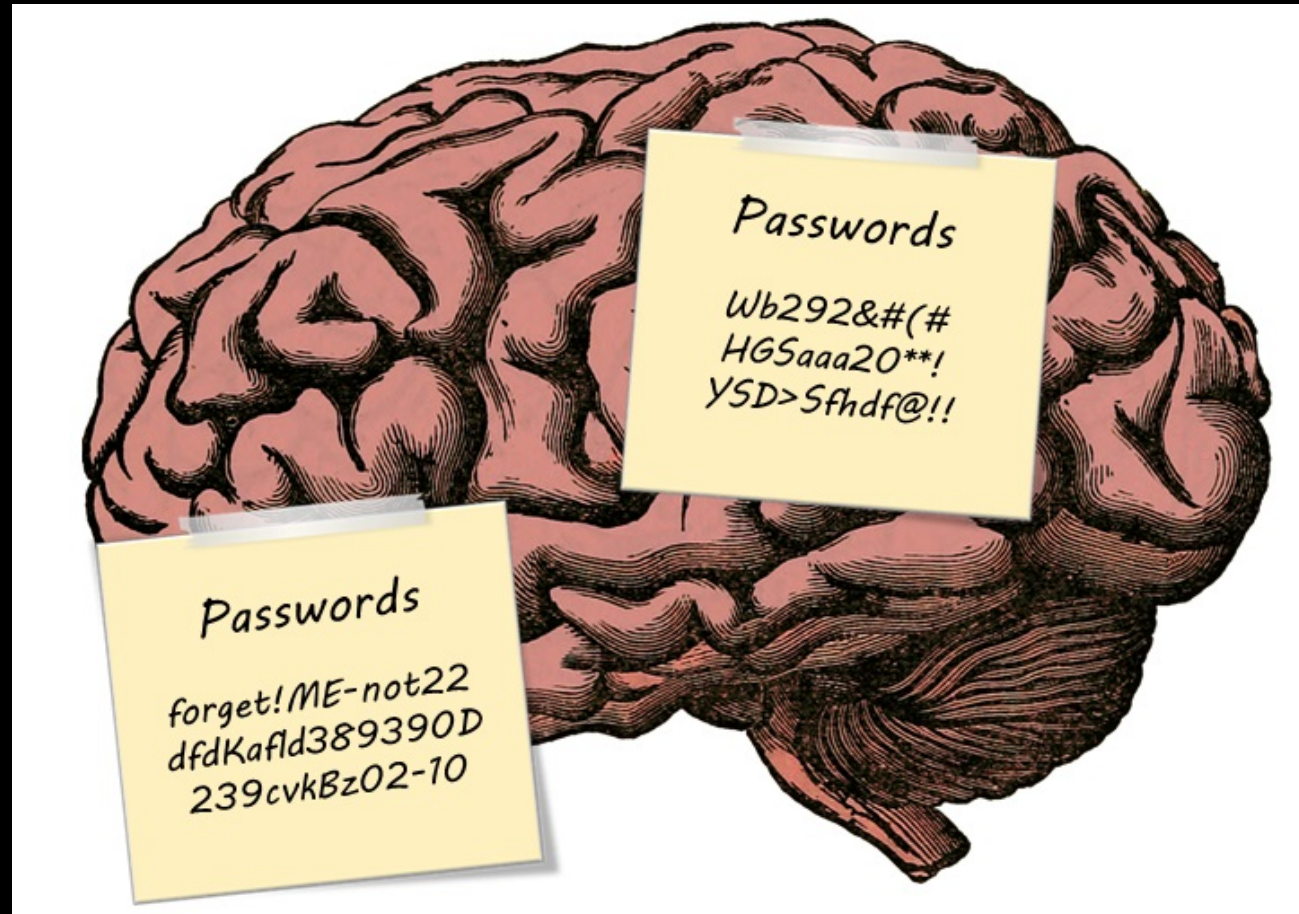
- Pick 4 random words
 - Chicken + Blender + Airplane + Orange
- Pick 2 numbers
 - 9 + 0
- Pick 2 symbols
 - () – this is Shift + 90
- Lets put it all together
 - ChickenBlenderAirplaneOrange90()
- Wow, that's 32 characters!



Password Examples

- Facebook_stol3/my+datas
- Eat-mor*chikn#nugs
- ChickenSaladChair12!@
- ~NCAVA#Conf_isthebest~

But how do I remember all these passwords?



What is a Password Manager

- A vault for storing passwords
- Encrypts passwords with a master password
- Can generate random, long, complex, unique passwords for every site
- Online and offline options
 - Online options
 - Multi-device
 - Browser plugin
 - More accessible
 - Offline option
 - No internet requirement
 - Can be multi-device or stored on USB

Popular Password Managers

- Online
 - LastPass
 - 1Password
- Offline
 - KeePass2

LastPass ****



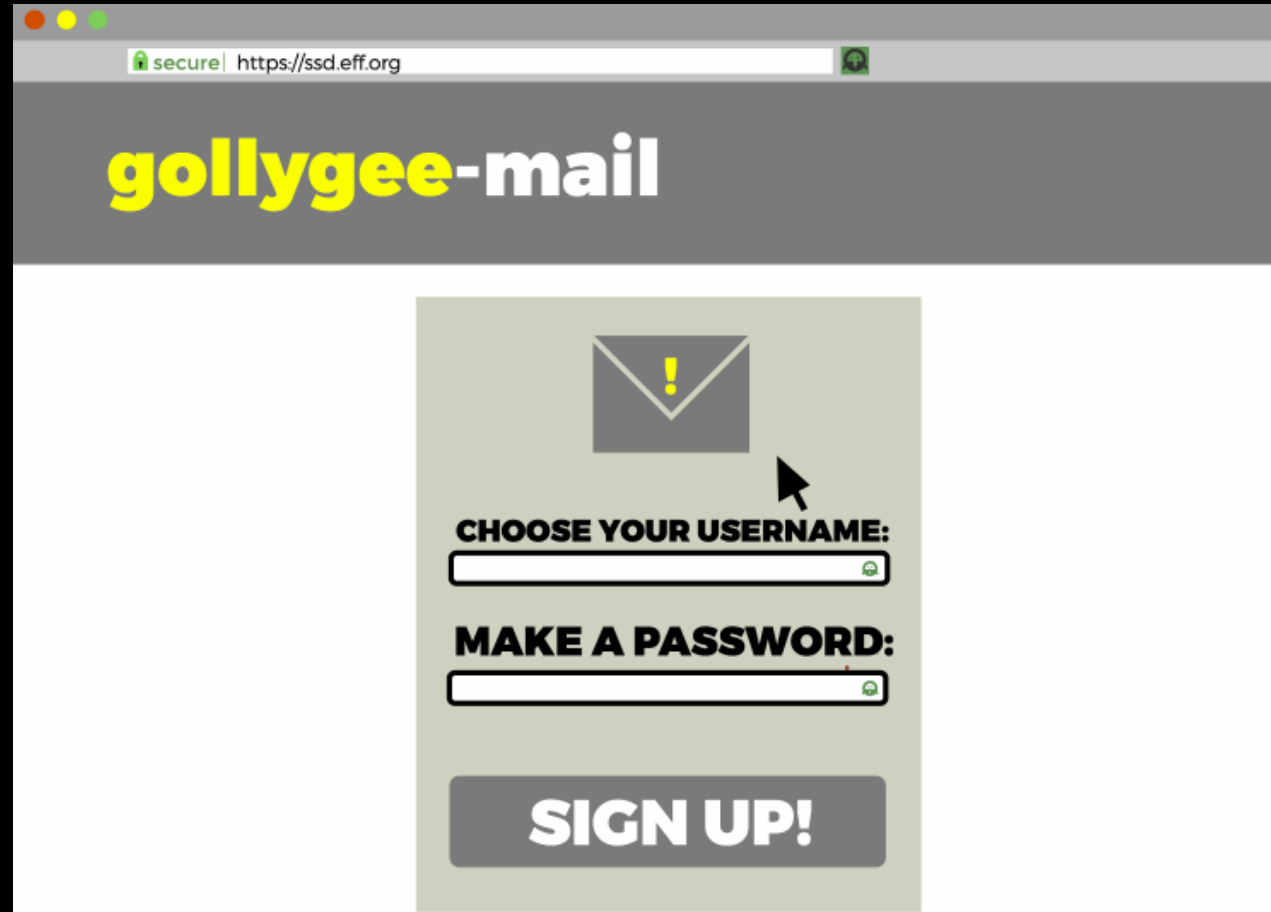
Password Manager Login

MR. PW MNGR

A cartoon character named Mr. PW MNGR. It has a round, light blue body with a darker blue outline. Its face is a light blue semi-circle with two small black dots for eyes and a simple curved line for a smile. Its torso is a darker blue semi-circle with a white keyhole in the center. It has two small, rounded arms and legs. A black mouse cursor arrow is pointing at the character's right side.

TYPE YOUR MASTER PASSWORD


Generating a Password



A screenshot of a web browser window showing the sign-up page for 'gollygee-mail'. The browser's address bar displays 'secure | https://ssd.eff.org'. The page has a grey header with the 'gollygee-mail' logo in yellow and white. The main content area is white and contains a central sign-up form with a light beige background. At the top of the form is an icon of an envelope with a yellow exclamation mark. Below this is the text 'CHOOSE YOUR USERNAME:' followed by a text input field with a green lock icon on the right. Underneath is the text 'MAKE A PASSWORD:' followed by another text input field with a green lock icon on the right. At the bottom of the form is a large grey button with the text 'SIGN UP!' in white.

secure | https://ssd.eff.org

gollygee-mail

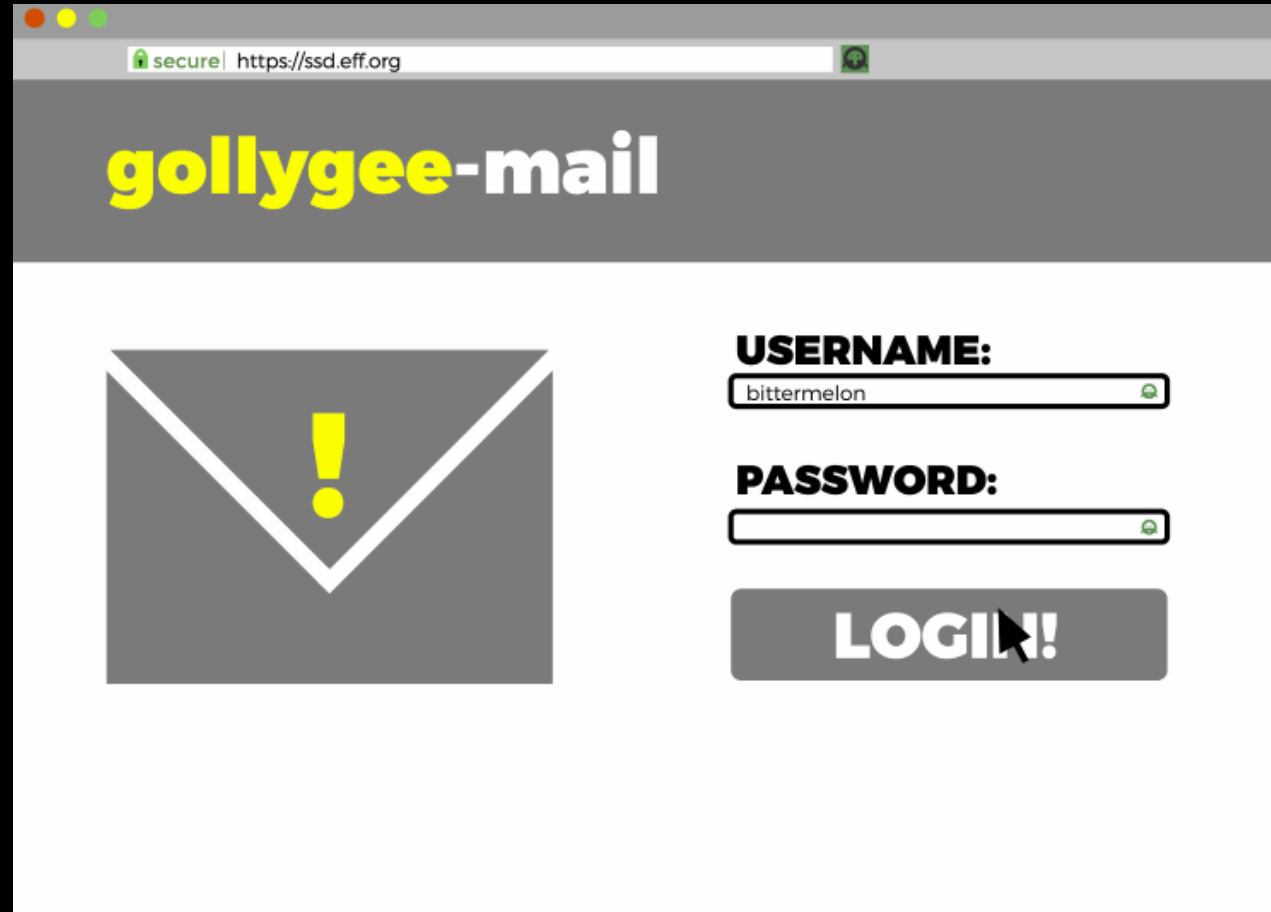


CHOOSE YOUR USERNAME:

MAKE A PASSWORD:

SIGN UP!


Pasting a Password



A screenshot of a web browser window showing the login page for "gollygee-mail". The browser's address bar displays "secure | https://ssd.eff.org". The page has a grey header with the site name in yellow and white. On the left is a large icon of a grey envelope with a yellow exclamation mark. On the right, there are two input fields: "USERNAME:" containing "bittermelon" and "PASSWORD:" which is empty. Both fields have a green lock icon on the right. Below the fields is a grey "LOGIN!!" button with a mouse cursor hovering over it.

secure | https://ssd.eff.org

gollygee-mail



USERNAME:

PASSWORD:

LOGIN!!

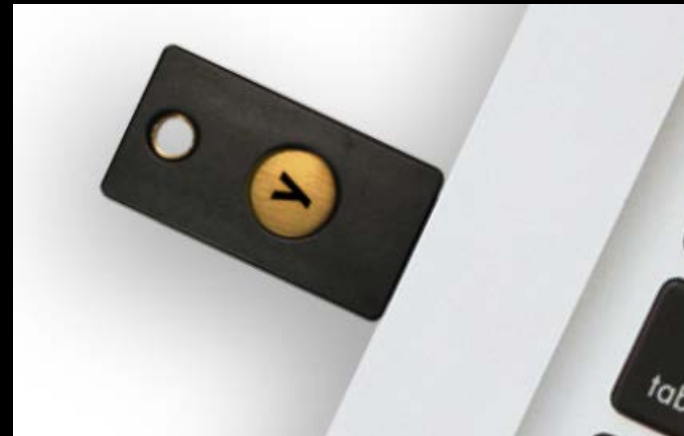
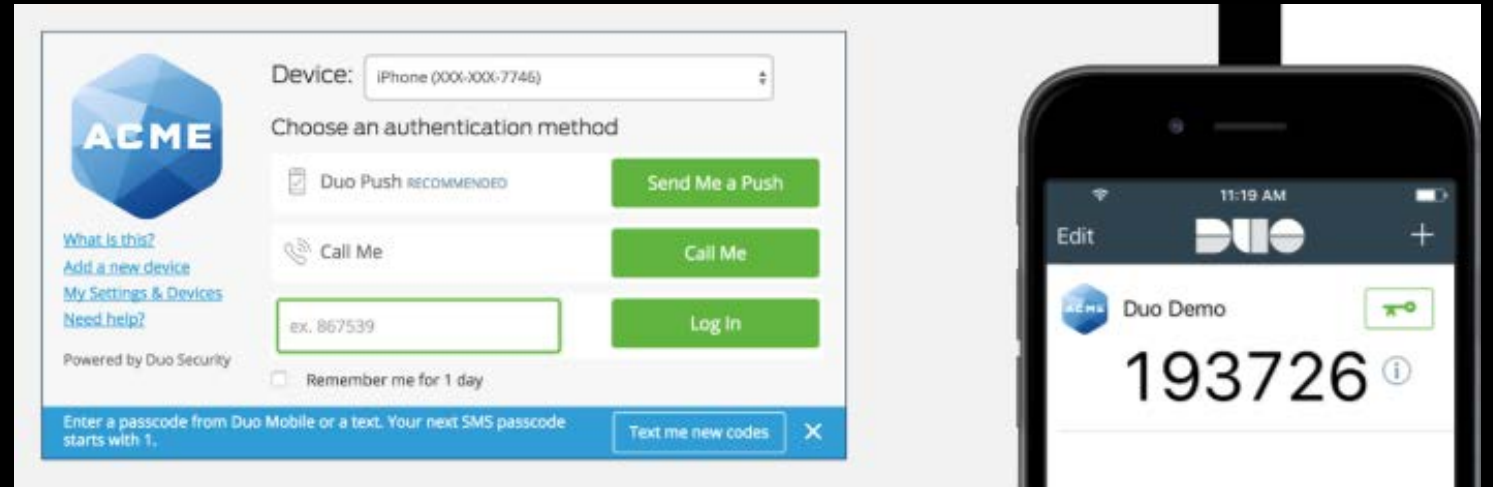
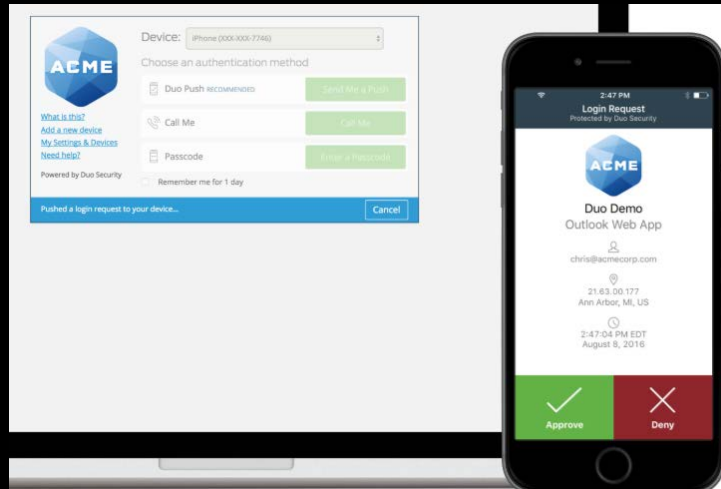
Multi Factor Authentication

- Many names: MFA, 2FA, multi-factor, two-factor
- What is it?
 - Something you are
 - Something you have
 - Something you know
- Why should I used it?
 - Protection if password is stolen
 - Not offered by all companies
 - <https://twofactorauth.org/>

MFA Options

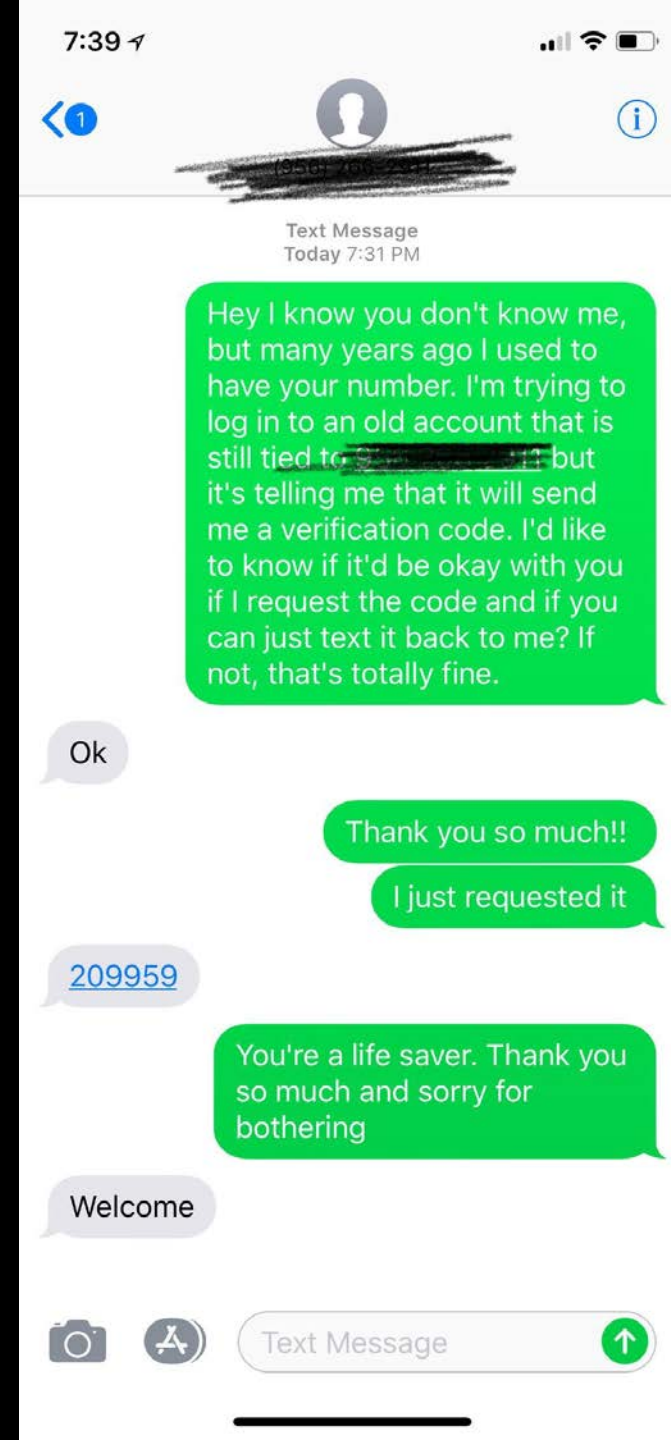
- Something you are
 - Retina scan, fingerprint, Facial recognition
- Something you have
 - OTP – One Time Passcode
 - SMS – Text message
 - Voice Call
 - Hardware token
 - Authenticator App
 - Hardware Key

MFA Options



New MFA Bypass

- Attacker gains user's credentials.
- Victim's account uses MFA.
- Attacker texts victim asking them to forward MFA code.
- Takes advantage of human nature.



Online Breach Dumps



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.

Breach date: 4 October 2013

Date added to HIBP: 4 December 2013

Compromised accounts: 152,445,165

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

```
4464-|--|-xxx@yahoo.com-|-g2B6PhWEH366cdBSCql/UQ==|-try: qwerty123|--
4465-|--|-xxxxx@jcom.home.ne.jp-|-Eh5tLomK+N+82csoVwU9bw==|-?????|--
4466-|--|-xx@hotmail.com-|-ahw2b2BELzgRTWYvQGn+kw==|-quiero a...|--
4467-|--|-xxx@yahoo.com-|-leMTcMPEPcjioxG6CatHBw==|-|--
4468-|-username-|-xxxxx@adobe.com-|-2GtbVrmsERzioxG6CatHBw==|-|--
4469-|--|-xxxxx@yahoo.com-|-4LSlo772tH4=-|-rugby|--
4470-|--|-xxx@hotmail.com-|-WXGzX56zRXnioxG6CatHBw==|-|--
4471-|--|-xxxx@yahoo.com-|-x3eI/bgfUNrioxG6CatHBw==|-myspace|--
4471-|--|-xxx@hotmail.com-|-kbyi9I8wDrrioxG6CatHBw==|-regular|--
```

Have I been pwned?

- <https://haveibeenpwned.com/>

';--have i been pwned?

Check if you have an account that has been compromised in a data breach

email address

pwned?

Account Privacy Settings

- By default, many sites make data public
- Review settings carefully, especially on social sites
- Sometimes can have unintended consequences
 - A perspective employer found my “private” pictures
 - My boss saw my online rant about how I hate my job
 - The burglar saw I was on vacation based on my insta-posted photos
 - My a business connection obtained my cell number

Example of Privacy Settings

facebook

Search

HomeProfileFind FriendsAccount

Choose Your Privacy Settings

Connecting on Facebook

Control basic information your friends will use to find you on Facebook. [View Settings](#)

Sharing on Facebook

These settings control who can see what you share.

Everyone	Everyone	Friends of Friends	Friends Only	Other
Friends of Friends	Your status, photos, and posts			*
Friends Only	Bio and favorite quotations			*
	Family and relationships			*
	Photos and videos you're tagged in			*
Recommended	Religious and political views			*
Custom	Birthday			*
	Permission to comment on your posts			*
	Places you check in to [?]			*
	Contact information			*
	<input checked="" type="checkbox"/> Let friends of people tagged in my photos and posts see them.			
	Customize settings			<input checked="" type="checkbox"/> This is your current setting.

Apps and Websites

Edit your settings for using apps, games and websites.

Block Lists

Edit your lists of blocked people and apps.

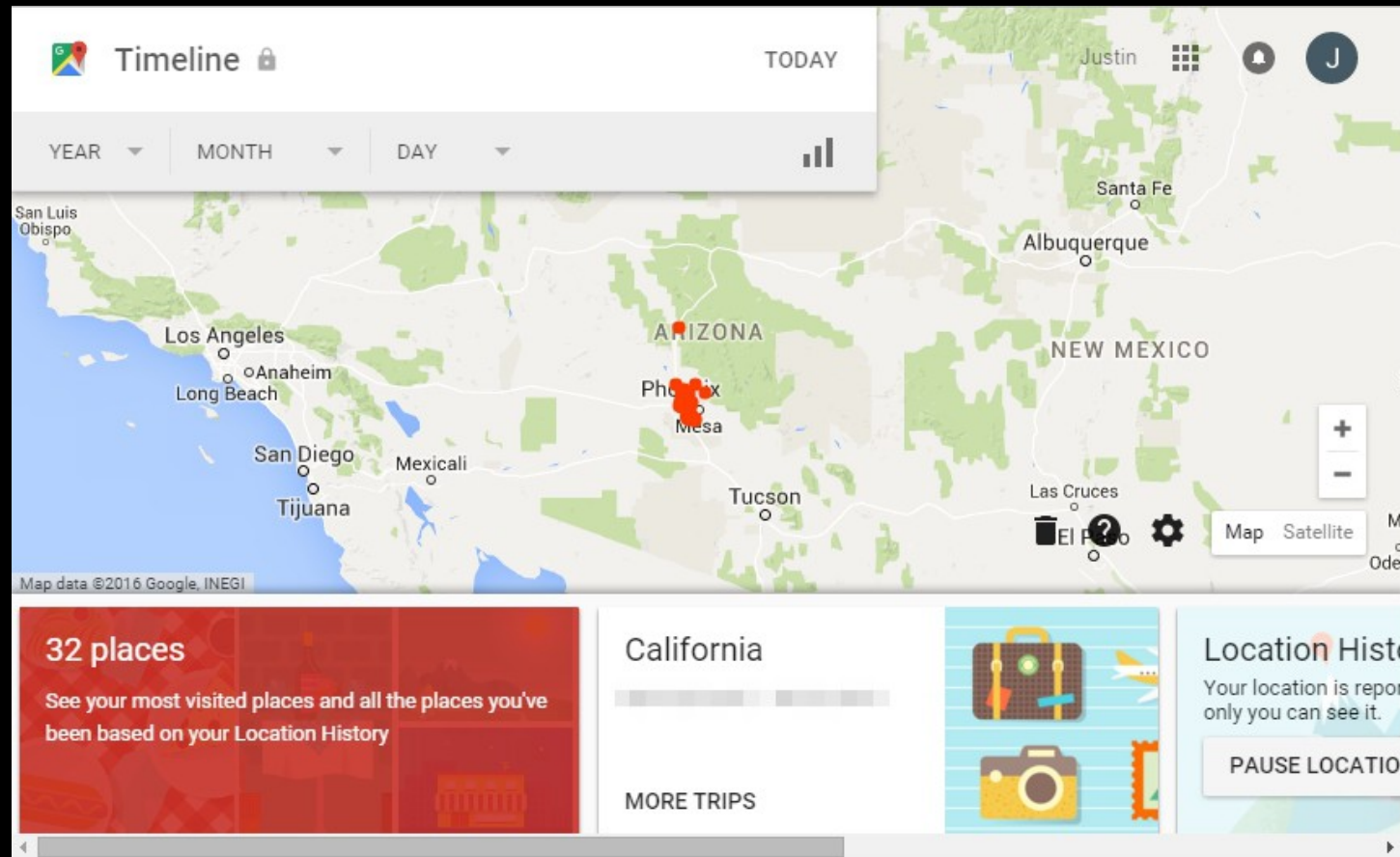
Controlling How You Share

[Learn more about your privacy on Facebook.](#)

Facebook © 2011 · English (US)About · Advertising · Create a Page · Developers · Careers · Privacy · Terms · Help

Google Account Timeline

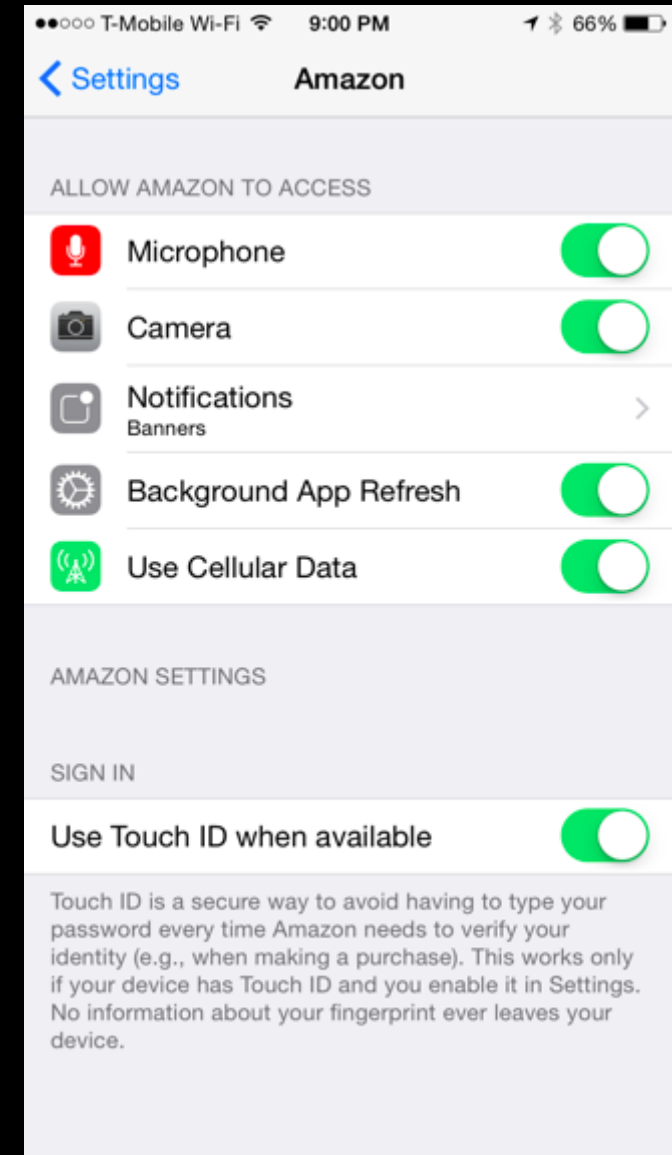
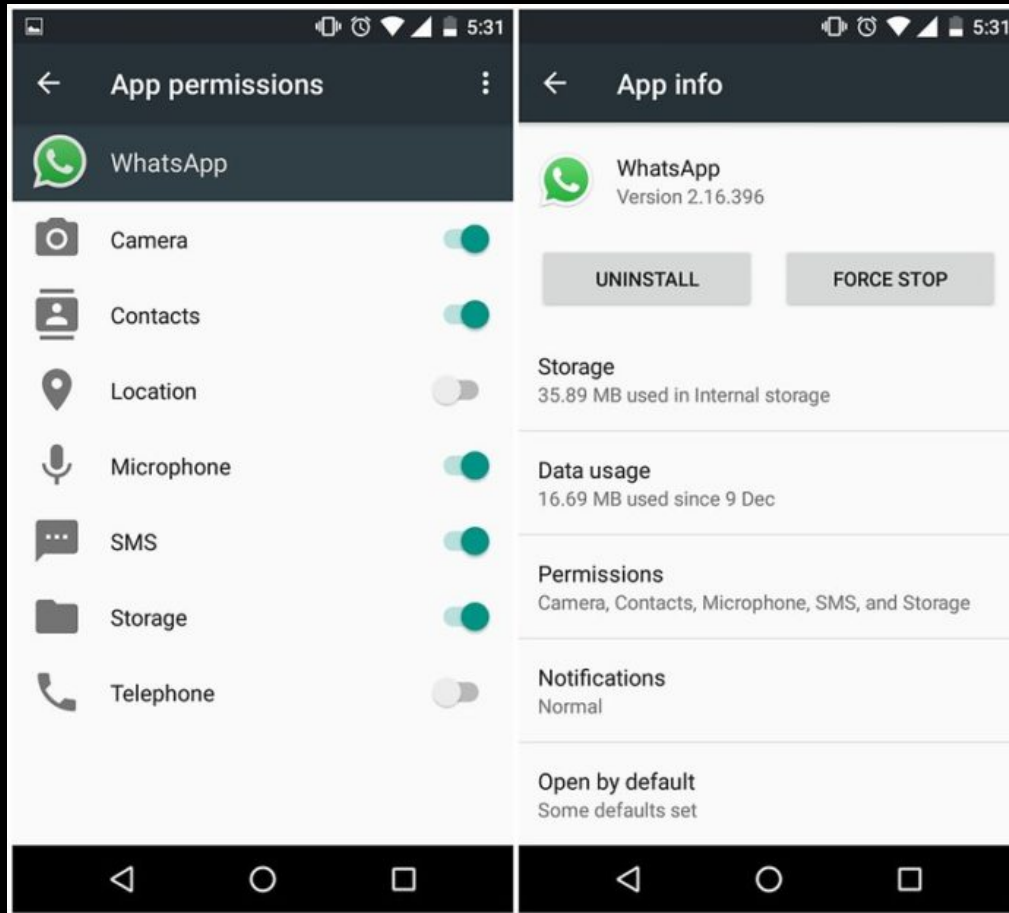
- <https://www.google.com/maps/timeline>



App Permissions

- Does my calculator app need access to my microphone?
- Why does my music app always want location services?
- When installing apps, be weary of the permissions they request
- Many newer devices have ability to retroactively control app permissions
- Check your mobile apps for any unusual settings.

App Permissions Example



Limit Personal Data Online

- Think before you post!
- What data are my apps collecting?
- What personal details am I posting to social media?
 - Out of wallet/ security question answers
 - Goldmine for identity theft/account compromise
 - Location data in posts?
- What else is out there?

Public Record Data

- Property Records
- Voter Records
- LinkedIn
- Social Media
- Organizations
- Google
- Data Agregators
 - Whitepages.com
 - Radaris.com

I want to Opt-out!

- Luckily there are options
- Great guides to help you get started
 - <https://tisiphone.net/2017/01/25/thwart-my-osint-efforts-while-binging-tv/>
 - <https://webbreacher.com/2017/04/24/removing-yourself-from-the-internet/>
- Phone Calls - <https://www.donotcall.gov/>
- Credit Offers - <https://www.optoutprescreen.com/>
- Direct Mail - <https://dmachoice.thedma.org/>

Device Security

How to I protect my devices?

- Phones
- Computers
- Tablets
- Lightbulbs
- Toys
- Toilets
- Everything is on the internet!?!?!?

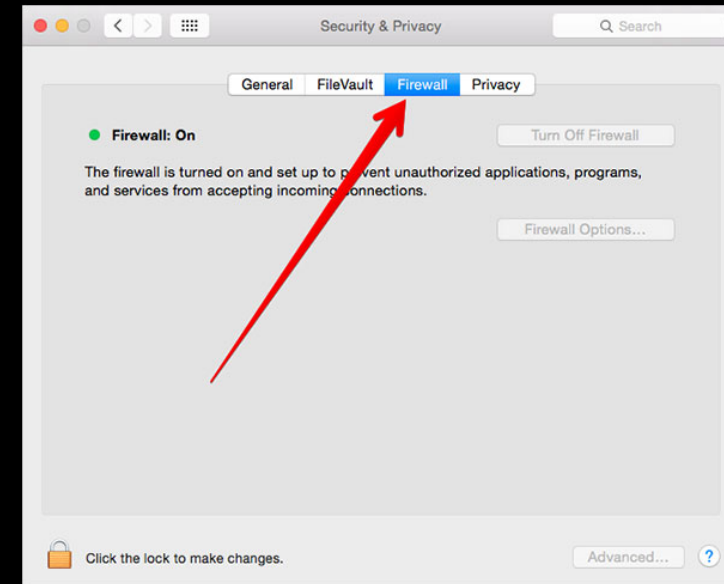
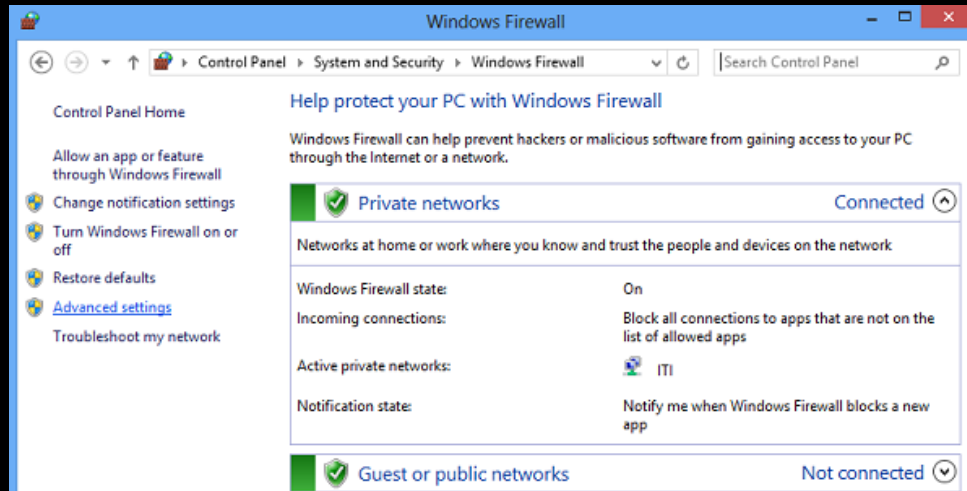


Credentials and Accounts

- Change default passwords – for EVERYTHING
 - IoT
 - Computers
 - TVs
 - Toilets
- Use separate accounts/devices for business/fun
- Use separate accounts/devices for kids/games
- Don't forget about 2-factor when applicable

Firewall

- Turn on local firewall
 - PC and Mac have built-in options for this
 - Turn on as restrictive as possible while still being usable



Updates

- Update all devices
 - Computers, phones, IoT, cars, etc.
- Turn on auto-updates
- Update all software
 - OS
 - Third party apps
- If you don't need it, uninstall it!

Antivirus

- Protects against malware
- Many free and paid options
- Some options include web filtering too
- Windows has a built in AV, Windows Defender
- Sophos has a free home version!

Adblockers

- An adblocker is a browser extension that limit the amount of ads that are displayed to you while browsing.
- Some debate on adblocker ethics
- Adblockers significantly reduce ad based malware
- Recommended extensions
 - AdBlock
 - uBlock Origin
- Other good extensions by EFF
 - Privacy Badger and HTTPS Everywhere

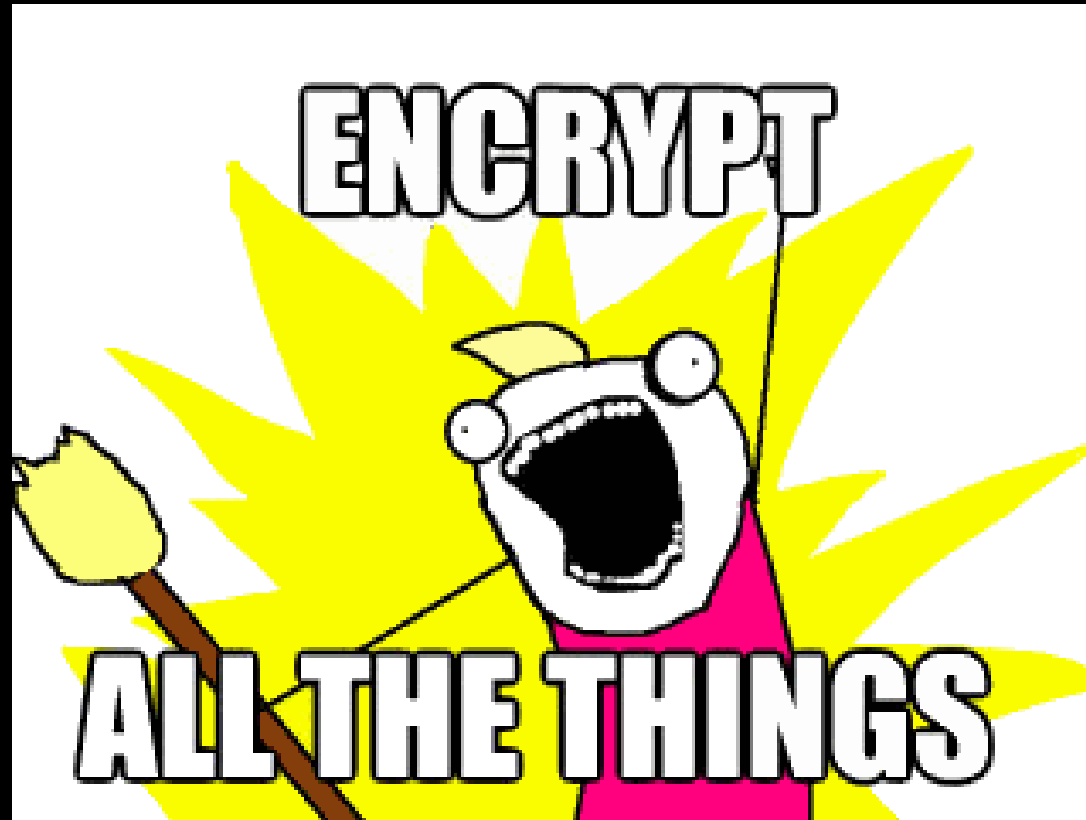
How do I backup my data?



Backup Solutions

- Online backups
 - Manual file backups (Google Drive, Dropbox, etc.)
 - Automatic backups (Carbonite, Backblaze, etc.)
- Offline backups options
 - CDs/DVDs
 - USB drive
 - External Hard drive
- Where do I store offline backups?

Encrypt your Backups!



Encryption Solutions

- Free
 - Paid
 - Software
 - Hardware
 - So many to choose!
-
- Don't lose your encryption key 😊

Software Encryption

- Open Source = Free + Time
 - Can be more difficult to use
 - Good for nerds and cheapskates
- Paid Solutions = \$\$\$
 - Typically easier to use
 - Better for average user
- How do I encrypt the cloud?

Hardware Encryption

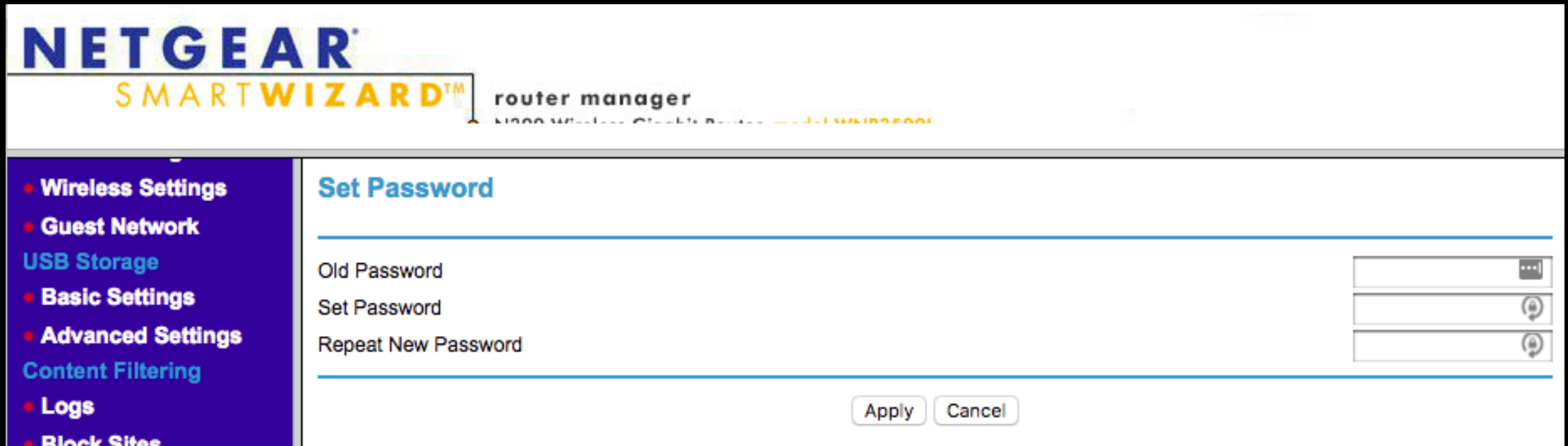
- Pre-built hardware
 - Easy to use, can be expensive
 - IronKey, Aegis Secure Key, etc.
- Make your own encrypted USB with VeraCrypt!



How do I secure my WiFi network?



Change default admin password



The image shows the Netgear Smart Wizard router manager interface. The top header features the "NETGEAR" logo in blue and "SMARTWIZARD™" in orange. Below this, "router manager" is written in a smaller font. A navigation menu on the left lists various settings: Wireless Settings, Guest Network, USB Storage, Basic Settings, Advanced Settings, Content Filtering, Logs, and Block Sites. The main content area is titled "Set Password" and contains three input fields: "Old Password", "Set Password", and "Repeat New Password". Each field has a small icon on the right side. At the bottom right of the form are "Apply" and "Cancel" buttons.

NETGEAR
SMARTWIZARD™ router manager

- Wireless Settings
- Guest Network
- USB Storage
- Basic Settings
- Advanced Settings
- Content Filtering
- Logs
- Block Sites

Set Password

Old Password

Set Password

Repeat New Password

Change SSID/WiFi Key

NETGEAR
SMARTWIZARD™ router manager

- Setup Wizard
- Add WPS Client
- Setup
 - Basic Settings
 - **Wireless Settings**
 - Guest Network
- USB Storage
 - Basic Settings
 - Advanced Settings
- Content Filtering
- Logs
- Block Sites
- Block Services
- Schedule
- E-mail
- Maintenance
 - Router Status
 - Attached Devices
 - Backup Settings
 - Set Password

Wireless Settings

Wireless Network

☒ Enable SSID Broadcast
☐ Enable Wireless Isolation

Name (SSID):

Region:

Channel:

Mode:

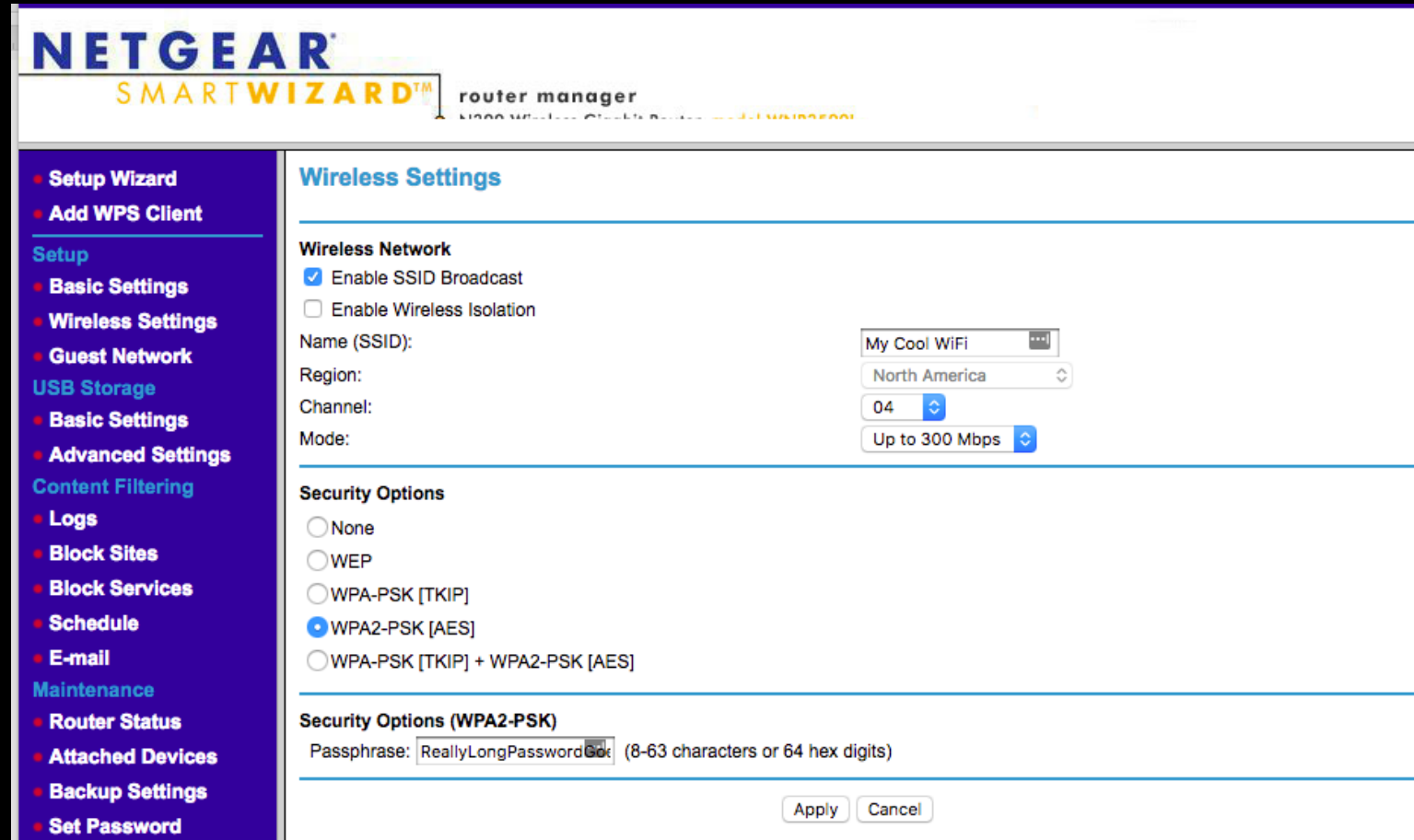
Security Options

☐ None
☐ WEP
☐ WPA-PSK [TKIP]
☒ WPA2-PSK [AES]
☐ WPA-PSK [TKIP] + WPA2-PSK [AES]

Security Options (WPA2-PSK)

Passphrase: (8-63 characters or 64 hex digits)

Use Strong Encryption WPA2-PSK



The screenshot shows the Netgear Smart Wizard router configuration interface. The left sidebar contains a navigation menu with categories like Setup, USB Storage, Content Filtering, Logs, Block Sites, Schedule, E-mail, and Maintenance. The main content area is titled 'Wireless Settings' and is divided into three sections: Wireless Network, Security Options, and Security Options (WPA2-PSK).

NETGEAR SMART WIZARD™ router manager

- Setup Wizard
- Add WPS Client
- Setup**
 - Basic Settings
 - **Wireless Settings**
 - Guest Network
- USB Storage**
 - Basic Settings
 - Advanced Settings
- Content Filtering**
 - Logs
 - Block Sites
 - Block Services
- Schedule**
- E-mail**
- Maintenance**
 - Router Status
 - Attached Devices
 - Backup Settings
 - Set Password

Wireless Settings

Wireless Network

☒ Enable SSID Broadcast
☐ Enable Wireless Isolation

Name (SSID):

Region:

Channel:

Mode:

Security Options

☐ None
☐ WEP
☐ WPA-PSK [TKIP]
☒ **WPA2-PSK [AES]**
☐ WPA-PSK [TKIP] + WPA2-PSK [AES]

Security Options (WPA2-PSK)

Passphrase: (8-63 characters or 64 hex digits)

Disable WPS

NETGEAR
SMARTWIZARD™ router manager

- Setup Wizard
- Add WPS Client
- Setup
 - Basic Settings
 - **Wireless Settings**
 - Guest Network
- USB Storage
 - Basic Settings
 - Advanced Settings
- Content Filtering
- Logs
- Block Sites
- Block Services
- Schedule
- E-mail
- Maintenance
 - Router Status
 - Attached Devices
 - Backup Settings
 - Set Password

Advanced Wireless Settings

Advanced Wireless Settings

☒ Enable Wireless Router Radio

Fragmentation Length (256-2346):

CTS/RTS Threshold (1-2347):

Preamble Mode

☐ Turn off wireless signal by schedule

The wireless signal is scheduled to turn off during the following time period:

Period	Start	End	Recurrence pattern
--------	-------	-----	--------------------

WPS Settings

Router's PIN: **66518624**

☒ Disable Router's PIN

☒ Keep Existing Wireless Settings

Wireless Card Access List

Use a Guest Network

NETGEAR
SMARTWIZARD™ router manager

Select Language:
English
Apply

• Setup Wizard

• Add WPS Client

Setup

• Basic Settings

• Wireless Settings

• Guest Network

USB Storage

• Basic Settings

• Advanced Settings

Content Filtering

• Logs

• Block Sites

• Block Services

• Schedule

• E-mail

Maintenance

• Router Status

• Attached Devices

• Backup Settings

• Set Password

• Router Upgrade

Advanced

• Wireless Settings

• Wireless Repeating Function

• Port Forwarding / Port Triggering

• WAN Setup

• LAN Setup

• QoS Setup

• Dynamic DNS

• Static Routes

• Remote Management

• UPnP

• IPv6

Guest Network Settings

Wireless Settings - Profile 1

☒ Enable Guest Network

☒ Enable SSID Broadcast

☐ Allow guest to access My Local Network

☒ Enable Wireless Isolation

Guest Wireless Network Name (SSID)

Security Options - Profile 1

☐ None

☐ WEP

☐ WPA-PSK [TKIP]

☒ WPA2-PSK [AES]

☐ WPA-PSK [TKIP] + WPA2-PSK [AES]

Security Options (WPA2-PSK)

Passphrase: (8-63 characters or 64 hex digits)

Apply

Cancel

Guest Network Settings

This is to allow visitors to use internet access at your home if you don't want to let them know your wireless security key.

Wireless Settings of Profile

Enable Guest Network

If this check box is checked, then this guest network is enabled. You and your visitors can connect to your network via the SSID of this profile.

Enable Wireless Isolation

If checked, the wireless client under this SSID can only access internet and it can't access other wireless clients even under the same SSID, Ethernet clients or this device. Other clients can't access the wireless client, either.

Enable SSID Broadcast

If Enabled, the Wireless Access Point will broadcast its name (SSID) to all Wireless Stations. Stations which have no SSID (or a null value) can then adopt the correct SSID for connections to this Access Point.

Allow Guest to access MY Local Network

If Unchecked, any user connects to this SSID can only access internet directly and other clients in the same SSID network. All clients in this SSID are not allowed to access router web GUI, clients of other SSIDs, Ethernet network and any other service of this Wireless Router.

If Checked, any user who connects to this SSID can access not only internet, but also local networks of this wireless router like users in primary SSID.

Guest Wireless Network Name (SSID)

Enter a value of up to 32 alphanumeric characters. The same Name (SSID) must be assigned to all wireless

Use OpenDNS DNS Servers

Domain Name Server (DNS) Address

☐ Get Automatically from ISP

☒ Use These DNS Servers


Primary DNS


208 . 67 . 222 . 222

Secondary DNS

208 . 67 . 220 . 220

=



 This domain is blocked due to content filtering.

Site blocked. gambling.com is not allowed on this network.

If you think this shouldn't be blocked, please [contact your network administrator](#).

This site was categorized in: **Gambling, Games**

D diagnostic Info

▼

OpenDNS Dashboard

OpenDNS.comDashboardCommunity

OpenDNS / dashboard

HOMESTATSETTINGSMY ACCOUNTSUPPORTTELL A FRIEND

Settings for:

– Select a network –

Dynamic IP addresses

OpenDNS supports networks ranging from single IP addresses, dynamic or static, on up to /16. [Learn more](#) about dynamic IPs.

Network verification

For individual IP addresses, verification is self-service, if you can click on a link from the network IP address. Networks larger than a single IP address are verified by OpenDNS employees reviewing account info and public records (like whois).

Add a network

IP:

4.14.30.234

Settings:

OpenDNS default settings

ADD THIS NETWORK

Your networks

LABEL	IP	STATS
Home	<div>174.99.109.124</div> <div>4.14.30.234</div>	<div></div> <div></div>

DELETE

Keep your network's IP up-to-date with our free software. Available for [Windows](#) and [Mac OS X](#).

Web Filtering and Security

Choose your filtering level

☐ **High** Protects against all adult-related sites, illegal activity, social networking sites, video sharing sites, and general time-wasters. 26 categories in this group - [View](#) - [Customize](#)

☐ **Moderate** Protects against all adult-related sites and illegal activity. 13 categories in this group - [View](#) - [Customize](#)

☐ **Low** Protects against pornography. 4 categories in this group - [View](#) - [Customize](#)

☐ **None** Nothing blocked.

☒ **Custom** Choose the categories you want to block.

<input type="checkbox"/> Academic Fraud	<input type="checkbox"/> Adult Themes	<input checked="" type="checkbox"/> Adware
<input type="checkbox"/> Alcohol	<input type="checkbox"/> Anime/Manga/Webcomic	<input type="checkbox"/> Auctions
<input type="checkbox"/> Automotive	<input type="checkbox"/> Blogs	<input type="checkbox"/> Business Services
<input type="checkbox"/> Chat	<input type="checkbox"/> Classifieds	<input checked="" type="checkbox"/> Dating
<input checked="" type="checkbox"/> Drugs	<input type="checkbox"/> Ecommerce/Shopping	<input type="checkbox"/> Educational Institutions
<input type="checkbox"/> File Storage	<input type="checkbox"/> Financial Institutions	<input type="checkbox"/> Forums/Message boards
<input checked="" type="checkbox"/> Gambling	<input type="checkbox"/> Games	<input type="checkbox"/> German Youth Protection
<input type="checkbox"/> Government	<input checked="" type="checkbox"/> Hate/Discrimination	<input type="checkbox"/> Health and Fitness
<input type="checkbox"/> Humor	<input type="checkbox"/> Instant Messaging	<input type="checkbox"/> Jobs/Employment
<input checked="" type="checkbox"/> Lingerie/Bikini	<input type="checkbox"/> Movies	<input type="checkbox"/> Music
<input type="checkbox"/> News/Media	<input type="checkbox"/> Non-Profits	<input checked="" type="checkbox"/> Nudity
<input type="checkbox"/> P2P/File sharing	<input type="checkbox"/> Parked Domains	<input type="checkbox"/> Photo Sharing
<input type="checkbox"/> Podcasts	<input type="checkbox"/> Politics	<input checked="" type="checkbox"/> Pornography
<input type="checkbox"/> Portals	<input checked="" type="checkbox"/> Proxy/Anonymizer	<input type="checkbox"/> Radio
<input type="checkbox"/> Religious	<input type="checkbox"/> Research/Reference	<input type="checkbox"/> Search Engines
<input checked="" type="checkbox"/> Sexuality	<input type="checkbox"/> Social Networking	<input type="checkbox"/> Software/Technology
<input type="checkbox"/> Sports	<input checked="" type="checkbox"/> Tasteless	<input type="checkbox"/> Television
<input type="checkbox"/> Tobacco	<input type="checkbox"/> Travel	<input type="checkbox"/> Video Sharing
<input type="checkbox"/> Visual Search Engines	<input checked="" type="checkbox"/> Weapons	<input type="checkbox"/> Web Spam
<input type="checkbox"/> Webmail		

Security

Malware/Botnet Protection ☒ **Enable basic malware/botnet protection**

When certain Internet-scale botnets are discovered or particularly malicious malware hits, we offer protection to all our users so that as many people as possible can be protected from the threat. At this time, this feature blocks the Conficker virus and the Internet Explorer Zero Day Exploit, and is continually expanded to include other types of malicious sites.

Phishing Protection ☒ **Enable phishing protection**

By enabling phishing protection, you'll protect everyone on your network from known phishing sites using the best data available.

Suspicious Responses ☐ **Block internal IP addresses**

When enabled, DNS responses containing IP addresses listed in [RFC1918](#) will be filtered out. This helps to prevent [DNS Rebinding attacks](#). For example, if `badstuff.attacker.com` points to `192.168.1.1`, this option would filter out that response.

The three blocks of IP addresses filtered in responses are:

```
10.0.0.0      - 10.255.255.255  (10/8)
172.16.0.0   - 172.31.255.255  (172.16/12)
192.168.0.0  - 192.168.255.255 (192.168/16)
```

OpenDNS Stats

Domains

Domains for Personal Networks on 2017-03-21 or choose a range of days

Filter: View everything

Next →

RANK	DOMAIN	REQUESTS
1	*.akamaiedge.net	144
2	*.fbcdn.net	74
3	api-global.netflix.com	64
4	*.amazonaws.com	55
5	star.c10r.facebook.com	51
6	matt.c10r.facebook.com	44
7	*.l.google.com	43
8	*.doubleclick.net	40
9	*.akamai.net	38
10	cooper.logs.roku.com	36
11	*.mail.yahoo.com	34
12	www-cdn.icloud.com.akadns.net	33
13	www.google.com	30
14	p20-keyvalueservice.fe.apple-dns.net	28
15	time-ios.apple.com	28
16	star-mini.c10r.facebook.com	28
17	*.cloudfront.net	26
18	p20-ckdatabase.fe.apple-dns.net	23
19	api.roku.com	23
20	graph.facebook.com	23

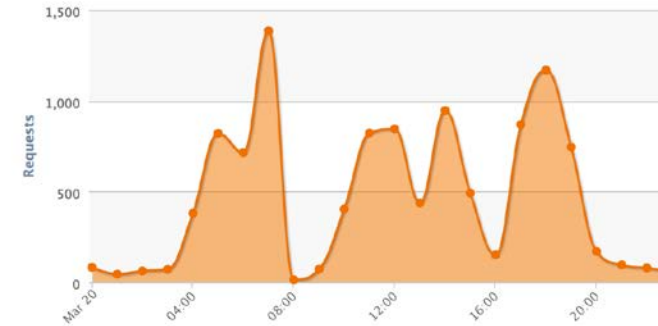
Domains

Domains for Personal Networks on 2017-03-20 or choose a range of days

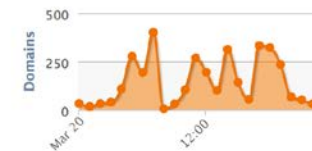
Filter: View only requests that were blocked

RANK	DOMAIN	REASON	REQUESTS
1	geo-um.btrll.com	Adware, ...	4
2	mobile.btrll.com	Adware, ...	2
3	vast.bp3871767.btrll.com	Adware, ...	2
4	gambling.com	Gambling, ...	1

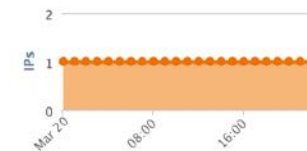
Recent Activity (all your networks, last day)



Unique Domains



Unique IPs



Request Types

Type	Requests
A	6744
SOA	5
PTR	7
TXT	19
AAAA	4060
SRV	125

Domains

Domain	Requests
*.akamaiedge.net	546
*.amazonaws.com	351
*.fbcdn.net	318
*.l.google.com	275
*.doubleclick.net	257
star.c10r.facebook.com	161

Securing WiFi - Recap

- Change default admin credentials
- Change default SSID
- Change default wireless key
- Use strong encryption
- Disable WPS
- Segment networks
- Use web filtering

Questions?



Thank you!

- Contact Info

- blak3irwin@gmail.com

- Slides and Resources

- <https://blak3irwin.github.io/>