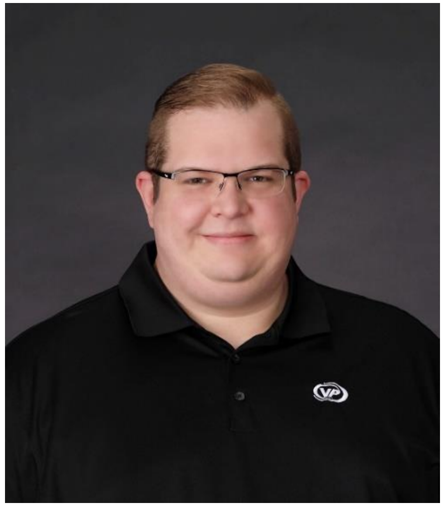
Mobile Threats & Data Access

Mobile Threat Protection and Defense Techniques

James Taylor
Sr. IT Security Consultant
Vantage Point Solutions
2211 N. Minnesota St.
Mitchell, SD 57301

(605) 995-1829
James.taylor@vantagepnt.com



Today's Speaker

James Taylor

Sr. IT Security Consultant

Vantage Point Solutions

About Me

- Father of 3 boys (18, 17, 15, my wife is a saint) and 2 dogs
- Graduate of Dakota State University, Bachelors Degrees in Computer Science (Information Security)
- Loves Capture The Flag (CTF is like a scavenger hunt with computers) competitions and gaming

Golden Age of Mobility

- In 2020, the number of smartphone **users** in the world is 5.17 Billion *
- By 2023 this number will **increase** to 7.33 Billion *
- There are 1.6 Billion more **mobile connections** than people worldwide. *

- * Statista website - https://www.statista.com/

Mobile Devices

- Make access and communication easier
- Allow for collaboration efforts between colleagues
- Store and share pictures, texts, videos and audio instantly
- Add efficiency and organization

- Could create health issues (blue light, sleep disfunctions, addictions, bacteria)
- Distraction and Stress causing
- Hard to know the exact permissions for files
- Insecure (Vulnerabilities)

Vulnerabilities'

- Given Common Vulnerability and Exposure number (CVE)
- CVE's assigned to all types of devices and software
- To date mobile vulnerabilities
  - 2500 Android
  - 1650 iOS (Apple)

Verizon Report

- Annually Verizon report detailing the state of mobile security
  - 3rd Edition
  - 800 Respondents in 11 industries
    - Almost 40% of organizations surveyed said they had experienced a mobile-related compromise
    - 66% of entities that suffered a breach said the impact was “major” and it was difficult and expensive to remediate
    - 45% of respondents admitted that their defenses were falling behind attackers’ capabilities

Breaches

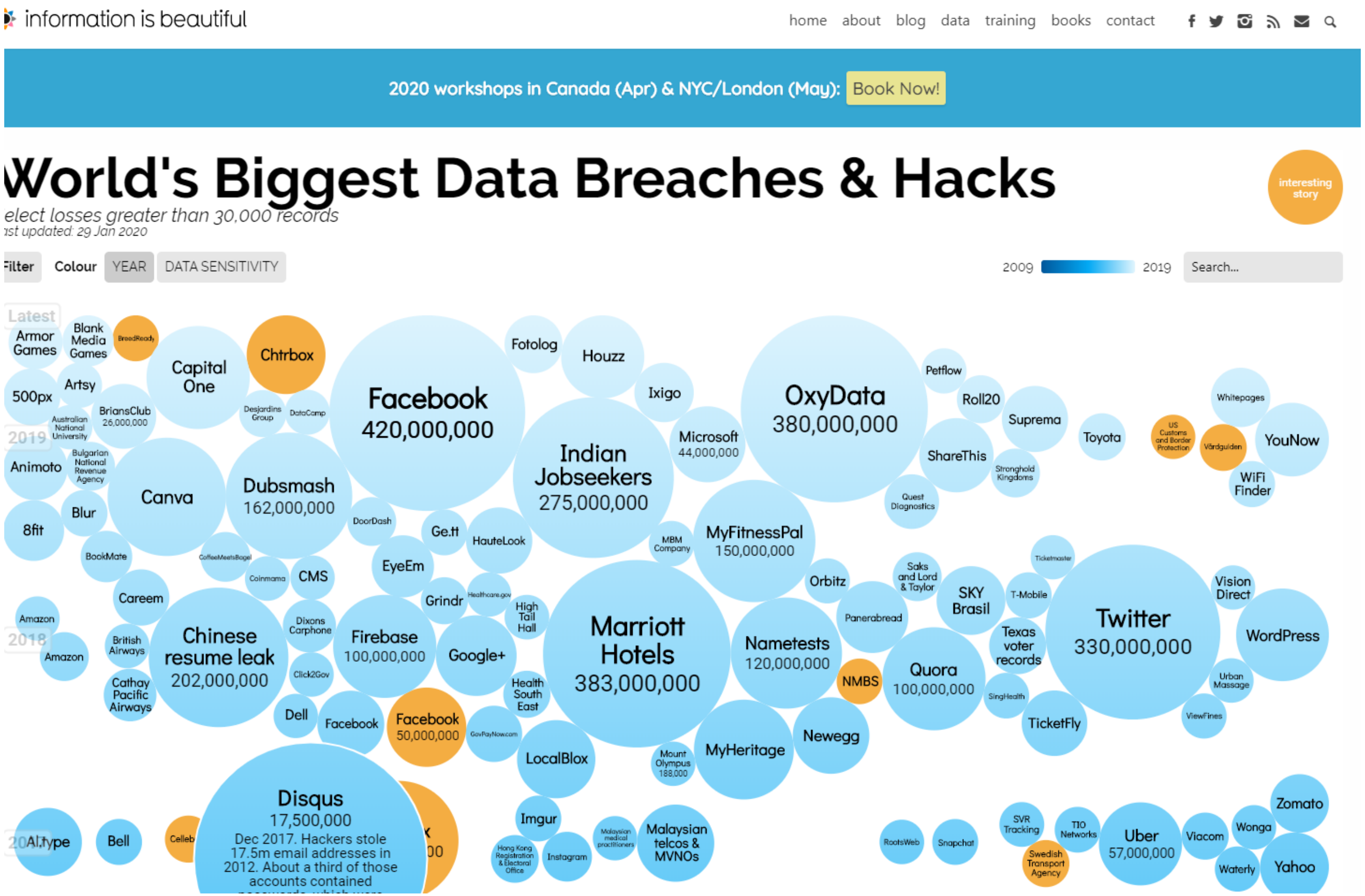
British Airways – 500,000 affected customers, cost BA 240 Million

My FitnessPal – 150 million accounts, contained username, email address, hashed password

Aadhaar – 1.1 **Billion** people affected, contained biometric data

Facebook – 420 Million accounts leaked

Breaches Cont….



information is beautiful

home about blog data training books contact

2020 workshops in Canada (Apr) & NYC/London (May): Book Now!

World's Biggest Data Breaches & Hacks

elect losses greater than 30,000 records

ıst updated: 29 Jan 2020

interesting story

Filter Colour YEAR DATA SENSITIVITY 2009 2019 Search...

Disqus 17,500,000 Dec 2017. Hackers stole 17.5m email addresses in 2012. About a third of those accounts contained

VantagePoint EMPLOYEE OWNED

Biggest Mobile threats today/future

UNSECURED WI-FI

PHISHING (SOCIAL ENGINEERING)

WEAK OR MISCONFIGURED SECURITY

DATA LEAKAGE

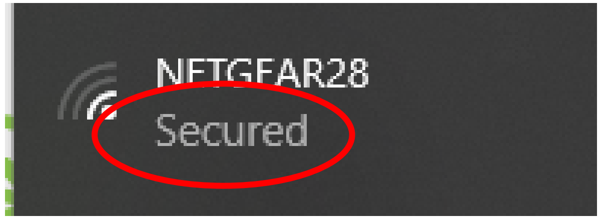
SIM JACKING

CRYPTO JACKING

Unsecured Wi-Fi

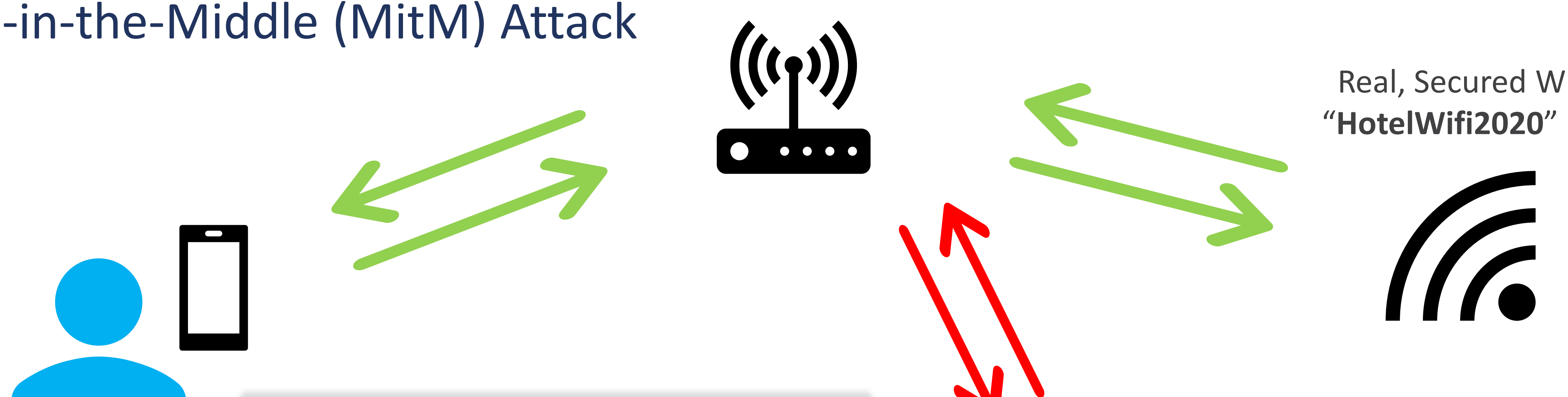
- Two types of Wi-Fi
  - Secured - requires authentication to login
  - Unsecured – requires no authentication to login
  - Possible Attacks:
    - Man-in-the-middle Attack
    - Evil Twin

Unsecured Wi-Fi Cont…



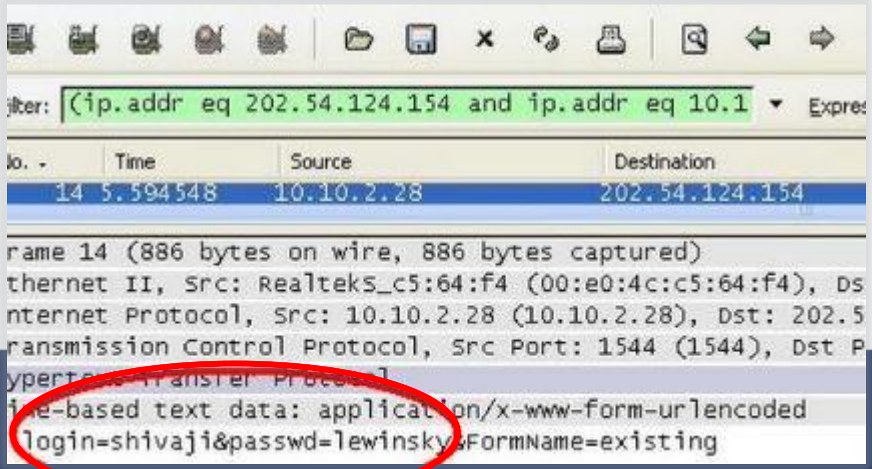
NETGEAR28
Secured

Man-in-the-Middle (MitM) Attack



Fake “Open” Wi-Fi Signal
“**hotelwifi2020**”

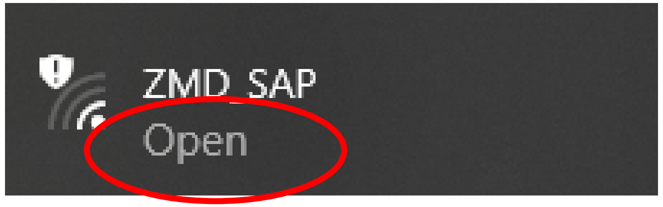
Real, Secured Wi-Fi Signal
“**HotelWifi2020**”



```
ilter: (ip.addr eq 202.54.124.154 and ip.addr eq 10.1   Expres

lo.    Time        Source          Destination
  14 5.594548     10.10.2.28      202.54.124.154

rame 14 (886 bytes on wire, 886 bytes captured)
thernet II, Src: RealtekS_c5:64:f4 (00:e0:4c:c5:64:f4), Ds
nternet Protocol, Src: 10.10.2.28 (10.10.2.28), Dst: 202.5
ransmission Control Protocol, Src Port: 1544 (1544), Dst P
ypertext Transfer Protocol
ine-based text data: application/x-www-form-urlencoded
 login=shivaji&passwd=lewinsky&FormName=existing
```

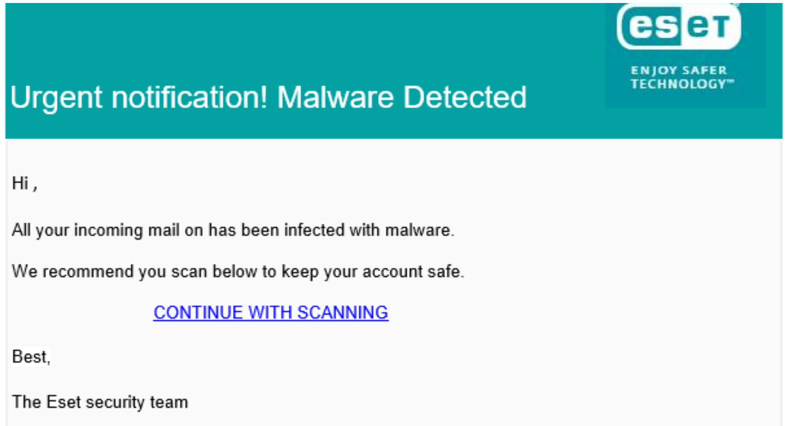


ZMD_SAP
Open

Phishing

- Easy way for malware/ransomware/spyware to enter the network
- Various Forms of attack
  - Phone calls
  - Emails
  - SMS/MMS (Text Messaging)
  - Voice (Calls and Voicemail)

Phishing Examples



Urgent notification! Malware Detected

eset ENJOY SAFER TECHNOLOGY™

Hi ,

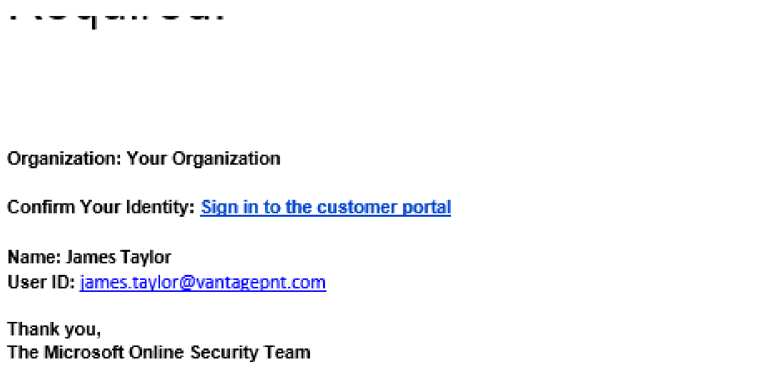
All your incoming mail on has been infected with malware.

We recommend you scan below to keep your account safe.

CONTINUE WITH SCANNING

Best,

The Eset security team



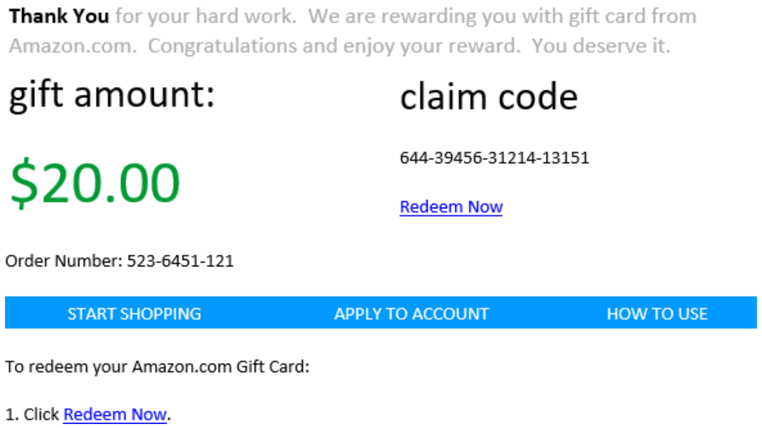
Required

Organization: Your Organization

Confirm Your Identity: Sign in to the customer portal

Name: James Taylor
User ID: james.taylor@vantagepnt.com

Thank you,
The Microsoft Online Security Team



Thank You for your hard work. We are rewarding you with gift card from Amazon.com. Congratulations and enjoy your reward. You deserve it.

gift amount: $20.00

claim code 644-39456-31214-13151

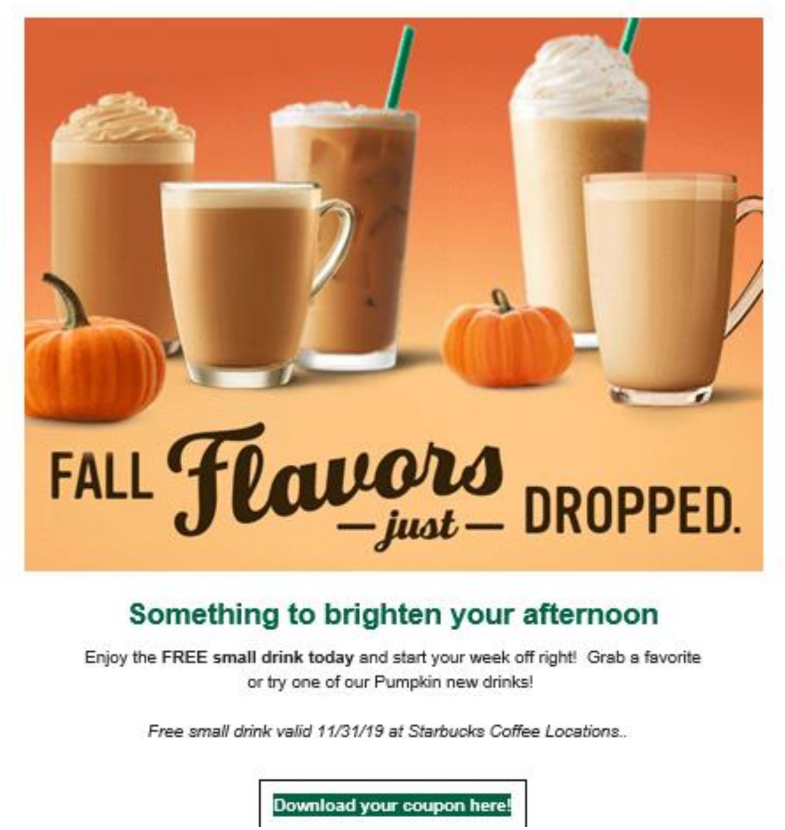
Redeem Now

Order Number: 523-6451-121

START SHOPPING APPLY TO ACCOUNT HOW TO USE

To redeem your Amazon.com Gift Card:

1. Click Redeem Now.

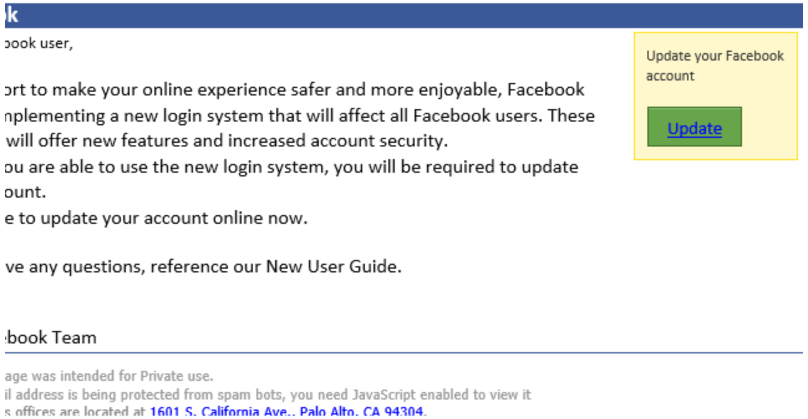


Something to brighten your afternoon

Enjoy the **FREE small drink today** and start your week off right! Grab a favorite or try one of our Pumpkin new drinks!

Free small drink valid 11/31/19 at Starbucks Coffee Locations..

Download your coupon here!



k

ɔook user,

ɔrt to make your online experience safer and more enjoyable, Facebook nplementing a new login system that will affect all Facebook users. These will offer new features and increased account security.
ou are able to use the new login system, you will be required to update ount.
e to update your account online now.

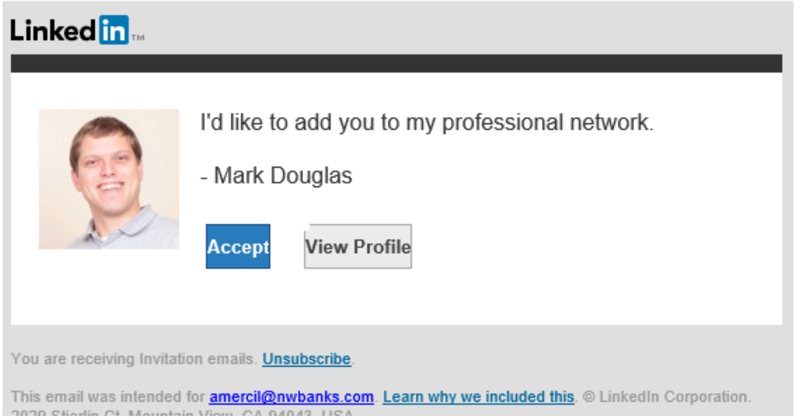
ve any questions, reference our New User Guide.

ːbook Team

Update your Facebook account

Update

age was intended for Private use.
il address is being protected from spam bots, you need JavaScript enabled to view it
s offices are located at 1601 S. California Ave., Palo Alto, CA 94304.



LinkedIn™

I'd like to add you to my professional network.

- Mark Douglas

Accept View Profile

You are receiving Invitation emails. Unsubscribe.

This email was intended for amercil@nwbanks.com. Learn why we included this. © LinkedIn Corporation. 2029 Stierlin Ct. Mountain View, CA 94043, USA

Social Engineering 101

And I can't remember what email address
we used to log on to the account,
and the baby's crying-
REAL FUTURE

Broken or Misconfigured Application Security

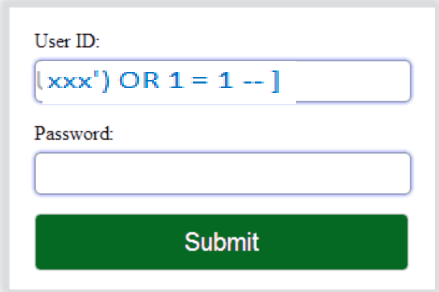
- A large amount of “broken” application in many ways
  - Misconfigurations
  - SQL Issues
  - Cross-site Scripting

VantagePoint
EMPLOYEE OWNED

Broken or Misconfigured Application Security Examples

SQL Injection

Malicious Actor
Discovers a website
with SQL Vulnerability

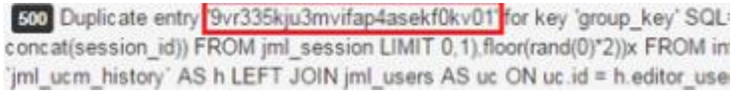


User ID:

[xxx') OR 1 = 1 --]

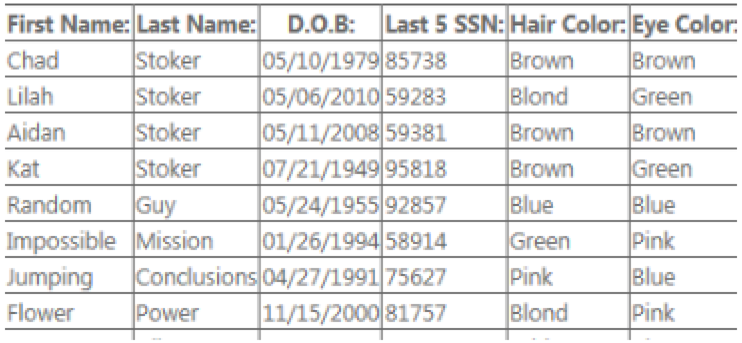
Password:

Website fails to
properly sanitize
database queries



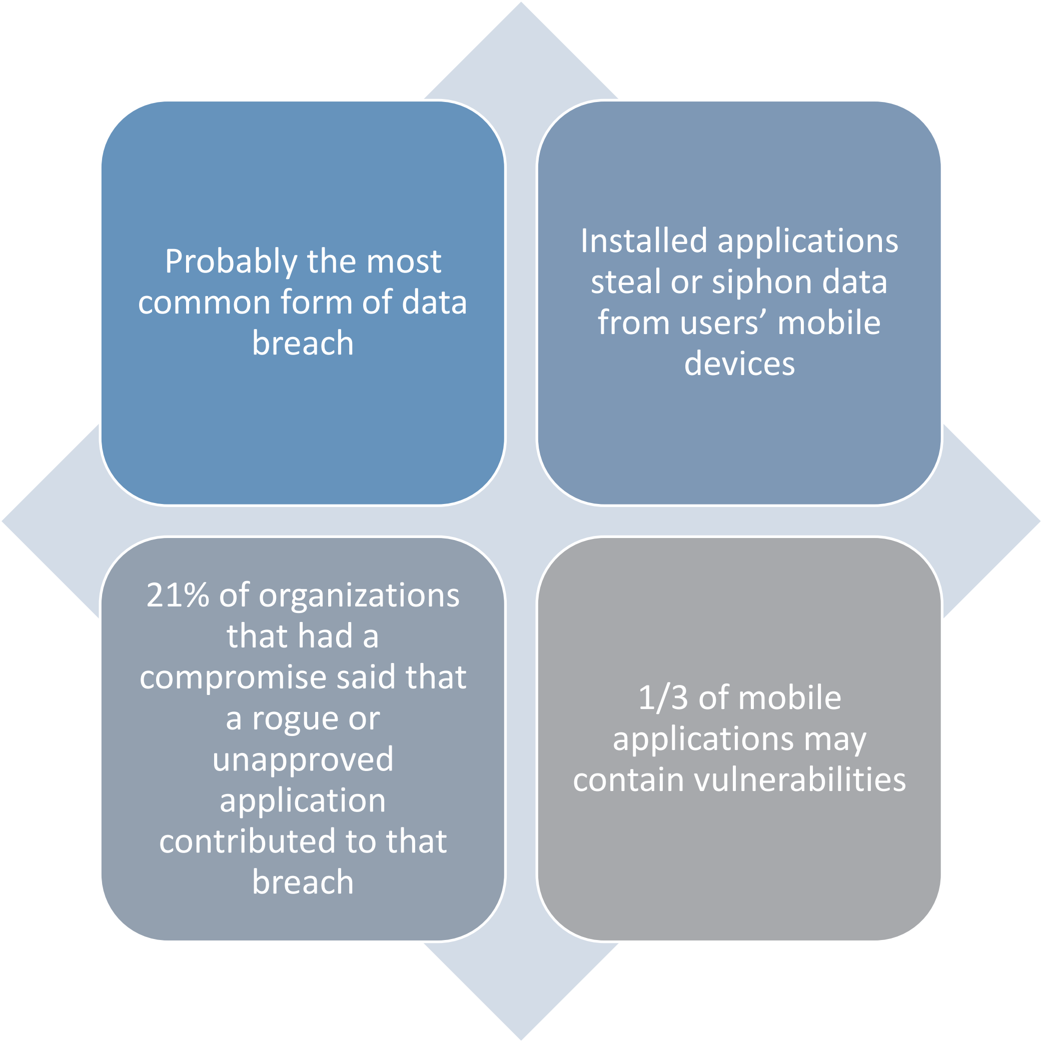
```
500 Duplicate entry '9vr335kju3mvifap4asekf0kv01' for key 'group_key' SQL:
concat(session_id)) FROM jml_session LIMIT 0,1),floor(rand(0)*2))x FROM in
`jml_ucm_history` AS h LEFT JOIN jml_users AS uc ON uc.id = h.editor_use
```

Website returns
the results of the
query



First Name:	Last Name:	D.O.B:	Last 5 SSN:	Hair Color:	Eye Color:
Chad	Stoker	05/10/1979	85738	Brown	Brown
Lilah	Stoker	05/06/2010	59283	Blond	Green
Aidan	Stoker	05/11/2008	59381	Brown	Brown
Kat	Stoker	07/21/1949	95818	Brown	Green
Random	Guy	05/24/1955	92857	Blue	Blue
Impossible	Mission	01/26/1994	58914	Green	Pink
Jumping	Conclusions	04/27/1991	75627	Pink	Blue
Flower	Power	11/15/2000	81757	Blond	Pink

Data Leakage



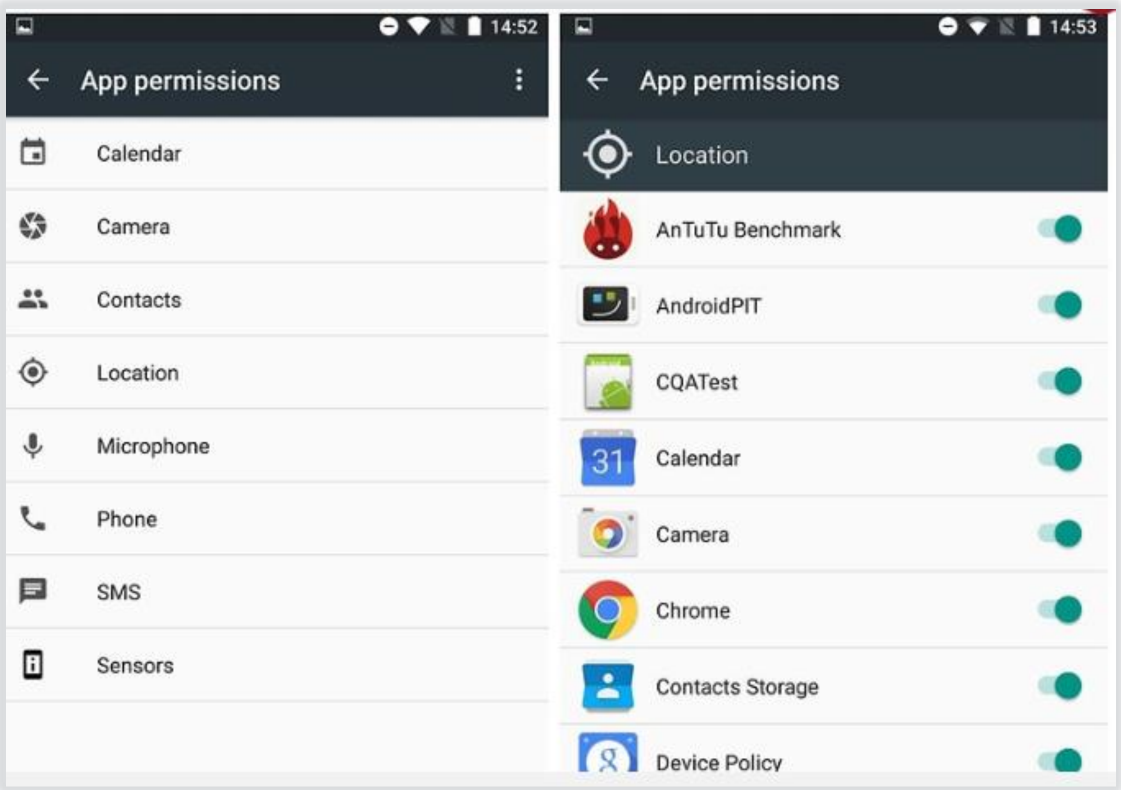
Probably the most common form of data breach

Installed applications steal or siphon data from users' mobile devices

21% of organizations that had a compromise said that a rogue or unapproved application contributed to that breach

1/3 of mobile applications may contain vulnerabilities

Data Leakage Example



14:52

App permissions

- Calendar
- Camera
- Contacts
- Location
- Microphone
- Phone
- SMS
- Sensors

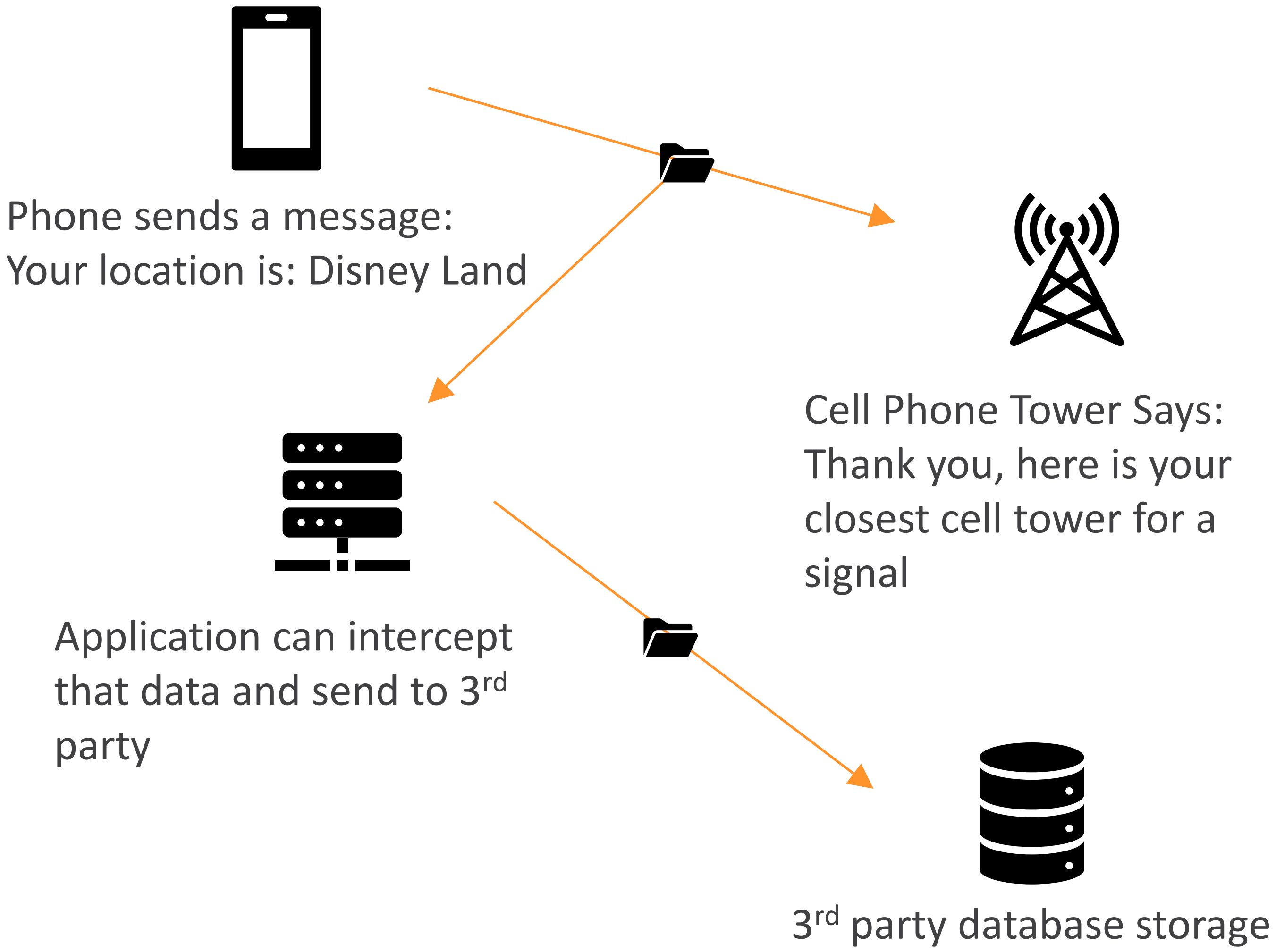
14:53

App permissions

Location

- AnTuTu Benchmark
- AndroidPIT
- CQATest
- Calendar
- Camera
- Chrome
- Contacts Storage
- Device Policy

Insecure Permissions



Phone sends a message:
Your location is: Disney Land

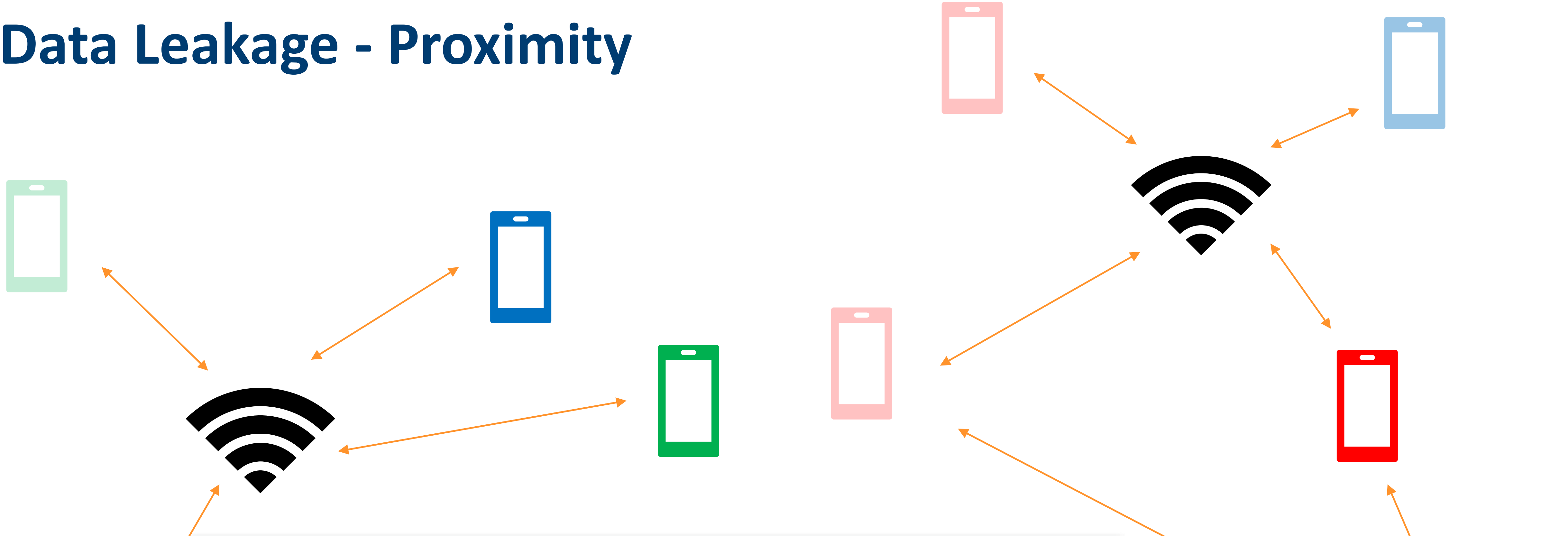
Cell Phone Tower Says: Thank you, here is your closest cell tower for a signal

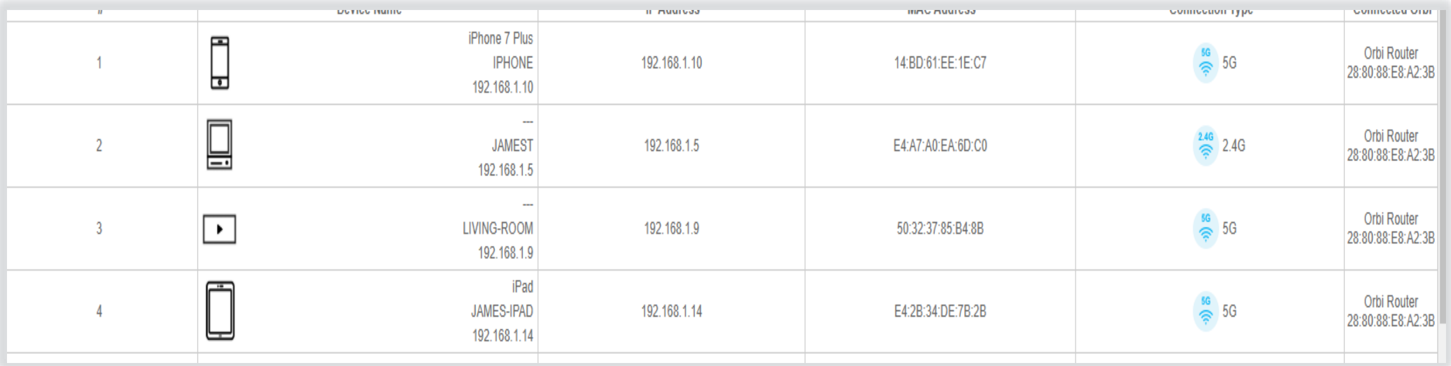
Application can intercept that data and send to 3rd party

3rd party database storage

Broadcast Activity

Data Leakage - Proximity



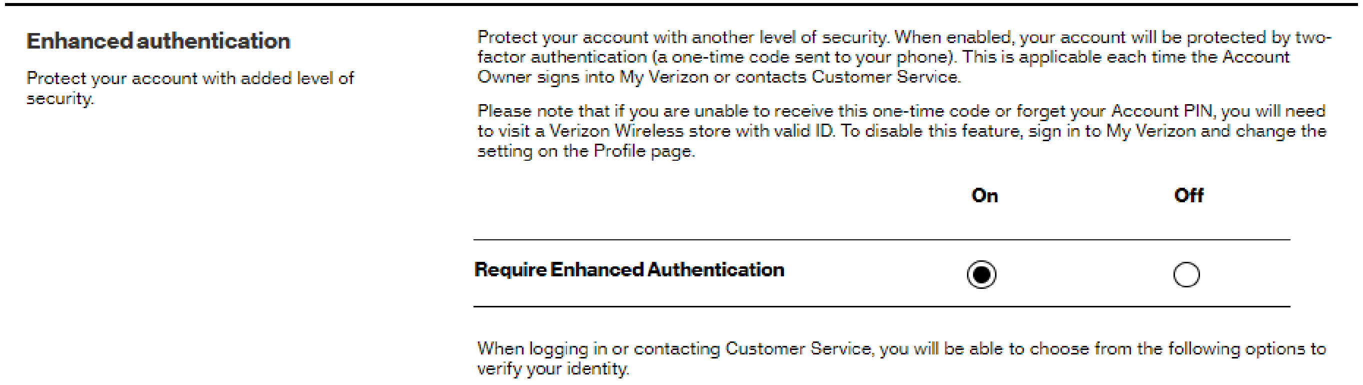


#	Device Name		IP Address	MAC Address	Connection Type	Connected Orbi
1	📱	iPhone 7 Plus IPHONE 192.168.1.10	192.168.1.10	14:BD:61:EE:1E:C7	5G	Orbi Router 28:80:88:E8:A2:3B
2	🖥	--- JAMEST 192.168.1.5	192.168.1.5	E4:A7:A0:EA:6D:C0	2.4G	Orbi Router 28:80:88:E8:A2:3B
3	▶	--- LIVING-ROOM 192.168.1.9	192.168.1.9	50:32:37:85:B4:8B	5G	Orbi Router 28:80:88:E8:A2:3B
4	📱	iPad JAMES-IPAD 192.168.1.14	192.168.1.14	E4:2B:34:DE:7B:2B	5G	Orbi Router 28:80:88:E8:A2:3B

Sim Jacking

- Technique done by transferring a phone number to a new sim card
- Attackers target the phone company using PII information to impersonate a real users
- Once done, can be used for the 2FA that is setup on that number

Sim Jacking Cont…



Enhanced authentication

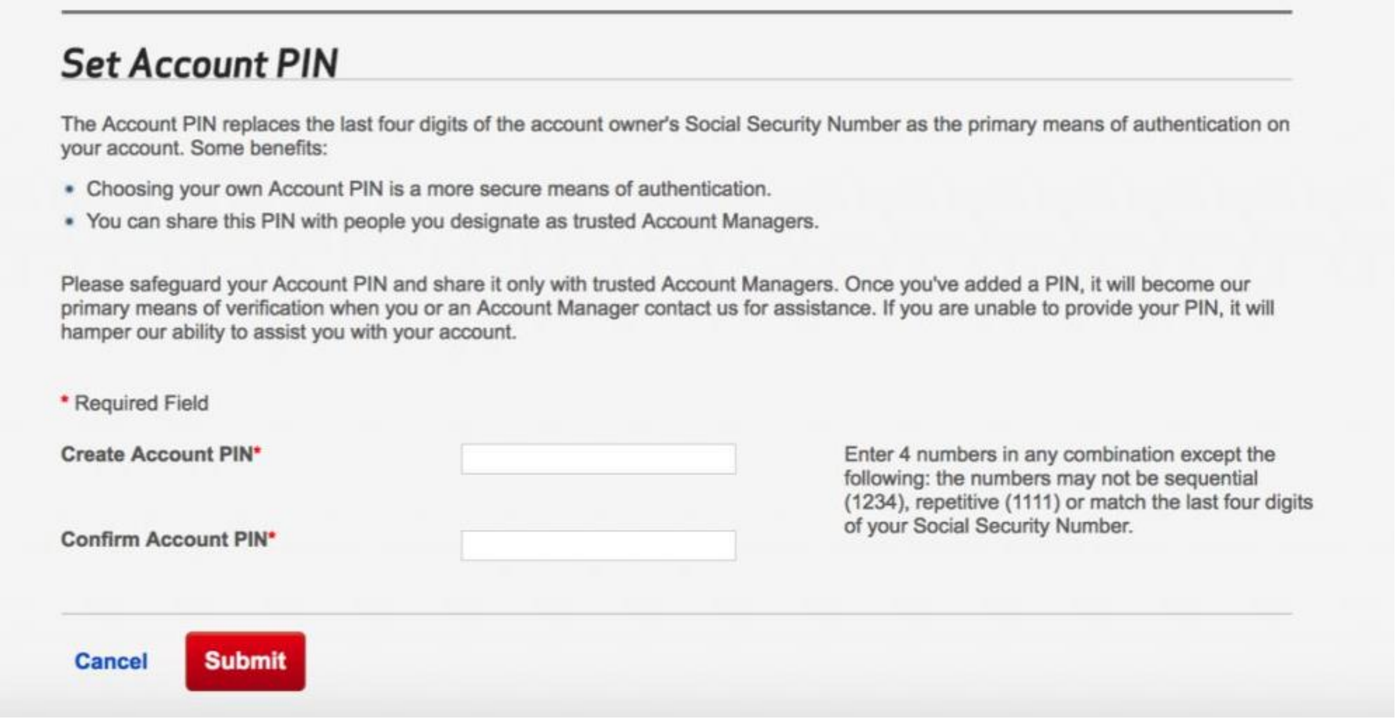
Protect your account with added level of security.

Protect your account with another level of security. When enabled, your account will be protected by two-factor authentication (a one-time code sent to your phone). This is applicable each time the Account Owner signs into My Verizon or contacts Customer Service.

Please note that if you are unable to receive this one-time code or forget your Account PIN, you will need to visit a Verizon Wireless store with valid ID. To disable this feature, sign in to My Verizon and change the setting on the Profile page.

	On	Off
Require Enhanced Authentication	●	○

When logging in or contacting Customer Service, you will be able to choose from the following options to verify your identity.



Set Account PIN

The Account PIN replaces the last four digits of the account owner's Social Security Number as the primary means of authentication on your account. Some benefits:

- Choosing your own Account PIN is a more secure means of authentication.
- You can share this PIN with people you designate as trusted Account Managers.

Please safeguard your Account PIN and share it only with trusted Account Managers. Once you've added a PIN, it will become our primary means of verification when you or an Account Manager contact us for assistance. If you are unable to provide your PIN, it will hamper our ability to assist you with your account.

* Required Field

Create Account PIN*

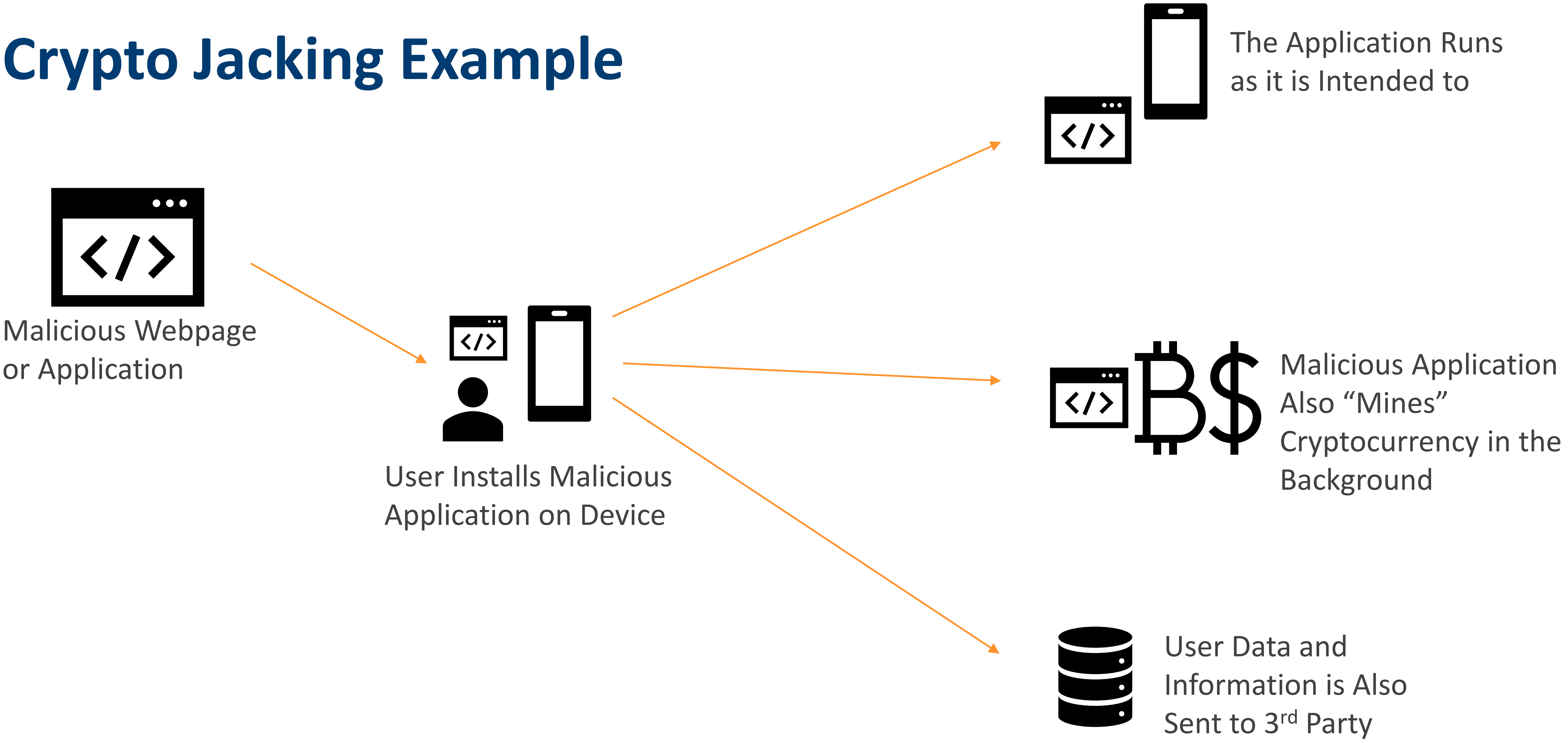
Confirm Account PIN*

Enter 4 numbers in any combination except the following: the numbers may not be sequential (1234), repetitive (1111) or match the last four digits of your Social Security Number.

Crypto Jacking

- Malicious website or application that “mine” for crypto currency
- User may not even be aware
- Can also farm data and information from devices

Crypto Jacking Example



Malicious Webpage or Application

User Installs Malicious Application on Device

The Application Runs as it is Intended to

Malicious Application Also “Mines” Cryptocurrency in the Background

User Data and Information is Also Sent to 3rd Party

How to Protect Your Mobile Data

- Updating
- Passwords
- Policies
- VPN
- 2FA

Updating

APPLY PATCHES AS THE ARE AVAILABLE

USE ONLY APPROVED APPLICATIONS ON THE APPROPRIATE AUTHORIZED STORE

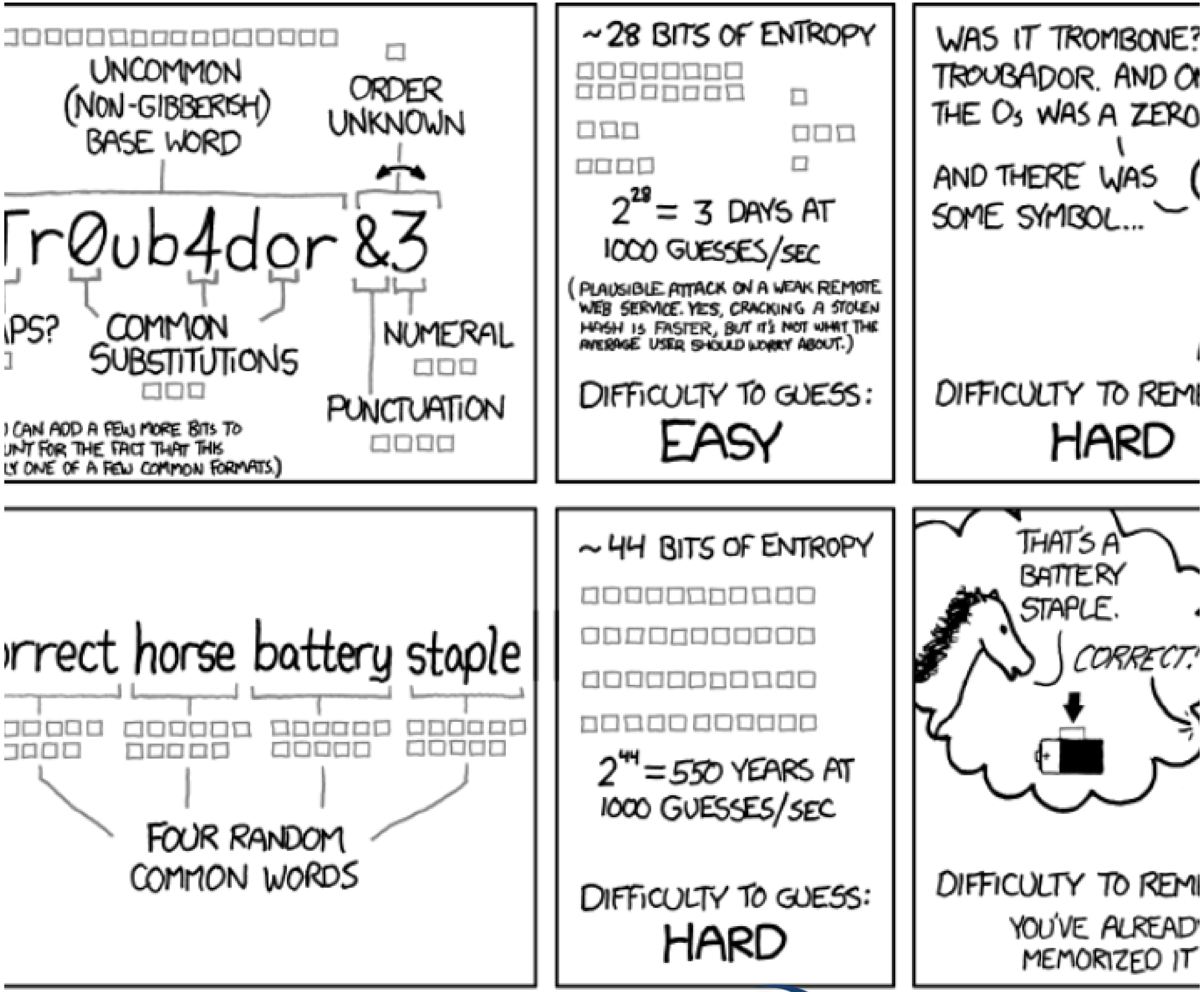
BLOCK JAVASCRIPT (MAY PROVE TROUBLESOME IN SOME CASES)

INSTALL PROGRAMS THAT PREVENT MINING (NO COIN, MINERBLOCK)

UPDATING POLICY AND PROGRAM FOR ALL DEVICES AND EQUIPMENT

Passwords

- Use of passphrases vs passwords
- Entropy
- correcthorsebatterystaple
- Password Managers
- Strict Password Policies


UNCOMMON (NON-GIBBERISH) BASE WORD
ORDER UNKNOWN
Tr0ub4dor &3
PS?
COMMON SUBSTITUTIONS
NUMERAL
PUNCTUATION
CAN ADD A FEW MORE BITS TO
UNT FOR THE FACT THAT THIS
LY ONE OF A FEW COMMON FORMATS.)
~28 BITS OF ENTROPY
2^28 = 3 DAYS AT 1000 GUESSES/SEC
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)
DIFFICULTY TO GUESS: EASY
WAS IT TROMBONE? TROUBADOR. AND ONE OF THE 0s WAS A ZERO
AND THERE WAS SOME SYMBOL...
DIFFICULTY TO REM
HARD
rrect horse battery staple
FOUR RANDOM COMMON WORDS
~44 BITS OF ENTROPY
2^44 = 550 YEARS AT 1000 GUESSES/SEC
DIFFICULTY TO GUESS: HARD
THAT'S A BATTERY STAPLE.
CORRECT!
DIFFICULTY TO REM
YOU'VE ALREAD MEMORIZED IT

Policies

- Mobile Security Policy
  - Comprehensive **Bring Your Own Device** policy
  - **Acceptable Use Policy** to dictate detailed usage
  - Detail Loss Mitigation Techniques
  - Employee training and testing of procedures

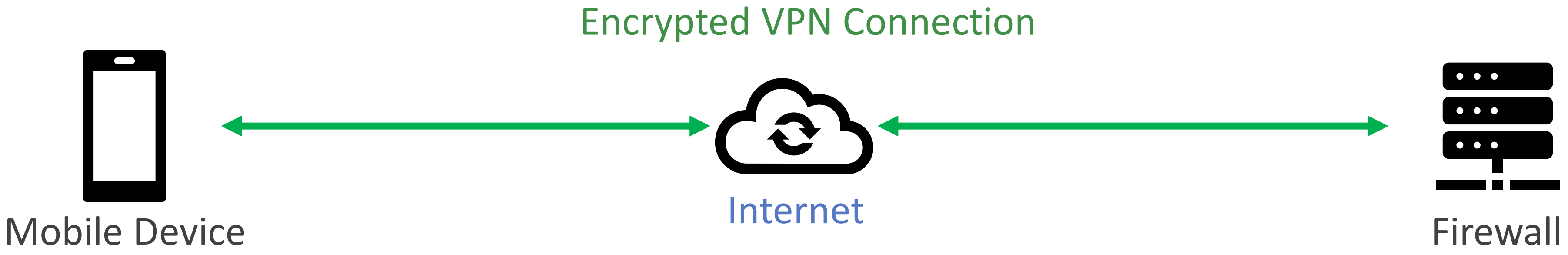
Other Security Mechanisms

Comprehensive Security Platform

- Manage Devices
- Data integration
- File and content filtering
- Remote lock and wipe
- Monitoring

VPN

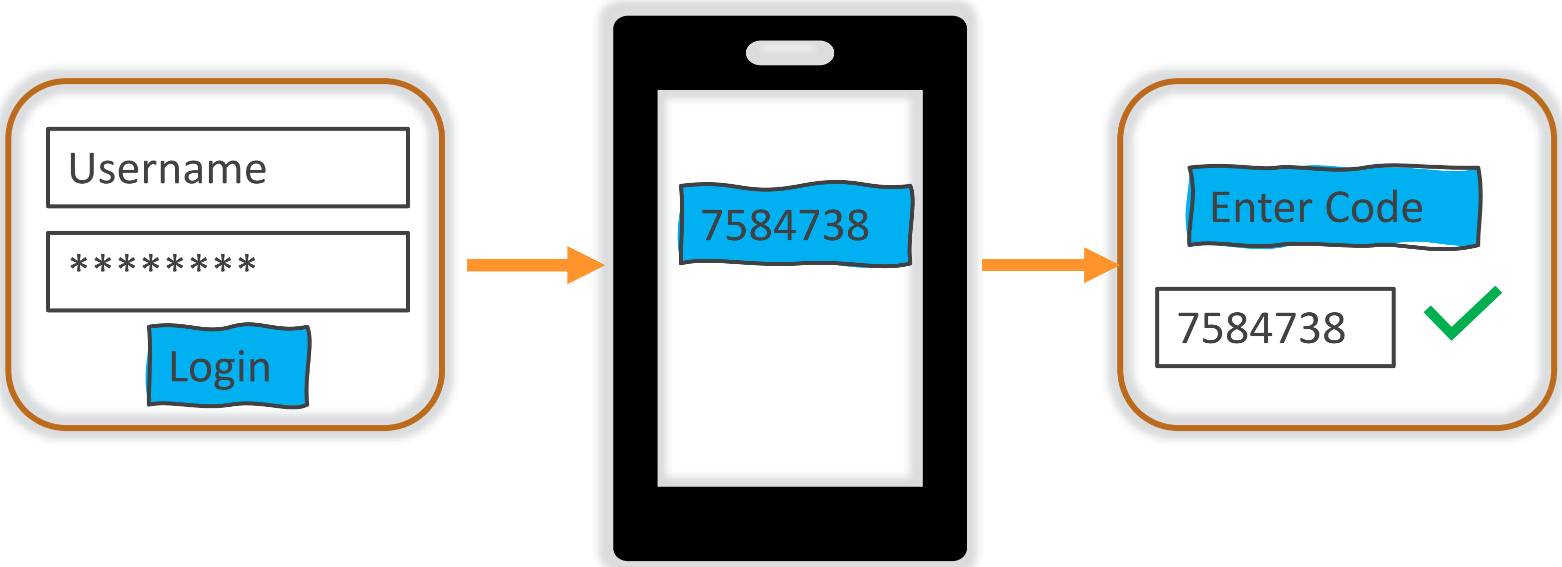
- Virtual Private Network (VPN) – encrypted connection over the internet to a server or firewall

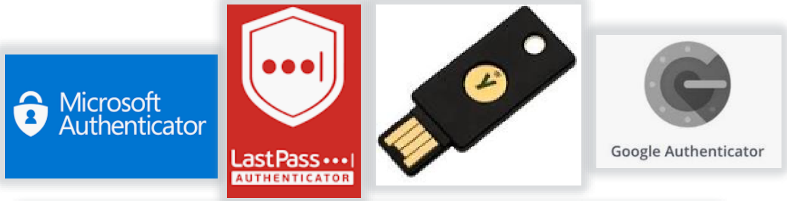


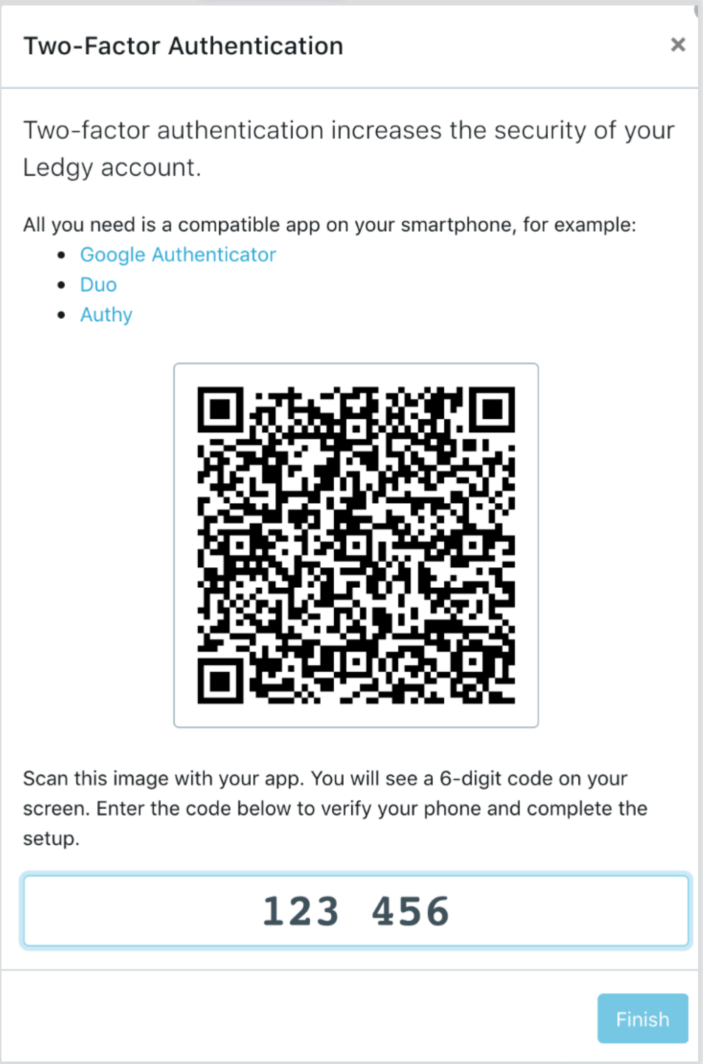
2FA

- Two-factor (2FA) or Multi-factor (MFA) authentication
- Additional source of verification for authorization
- Usually Username/Password and code from phone
- Not using “security questions” anymore

2FA Examples







Two-Factor Authentication

Two-factor authentication increases the security of your Ledgy account.

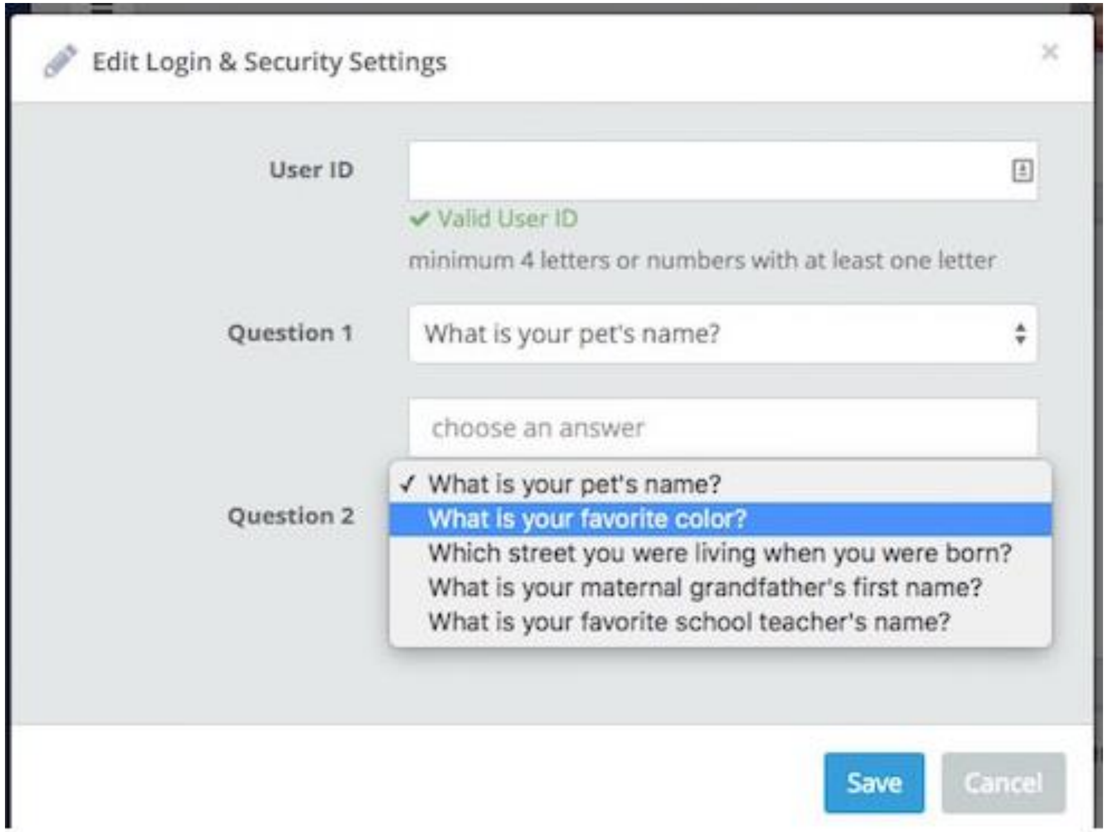
All you need is a compatible app on your smartphone, for example:

- Google Authenticator
- Duo
- Authy

Scan this image with your app. You will see a 6-digit code on your screen. Enter the code below to verify your phone and complete the setup.

123 456

Security Questions



Edit Login & Security Settings

User ID

✔ Valid User ID

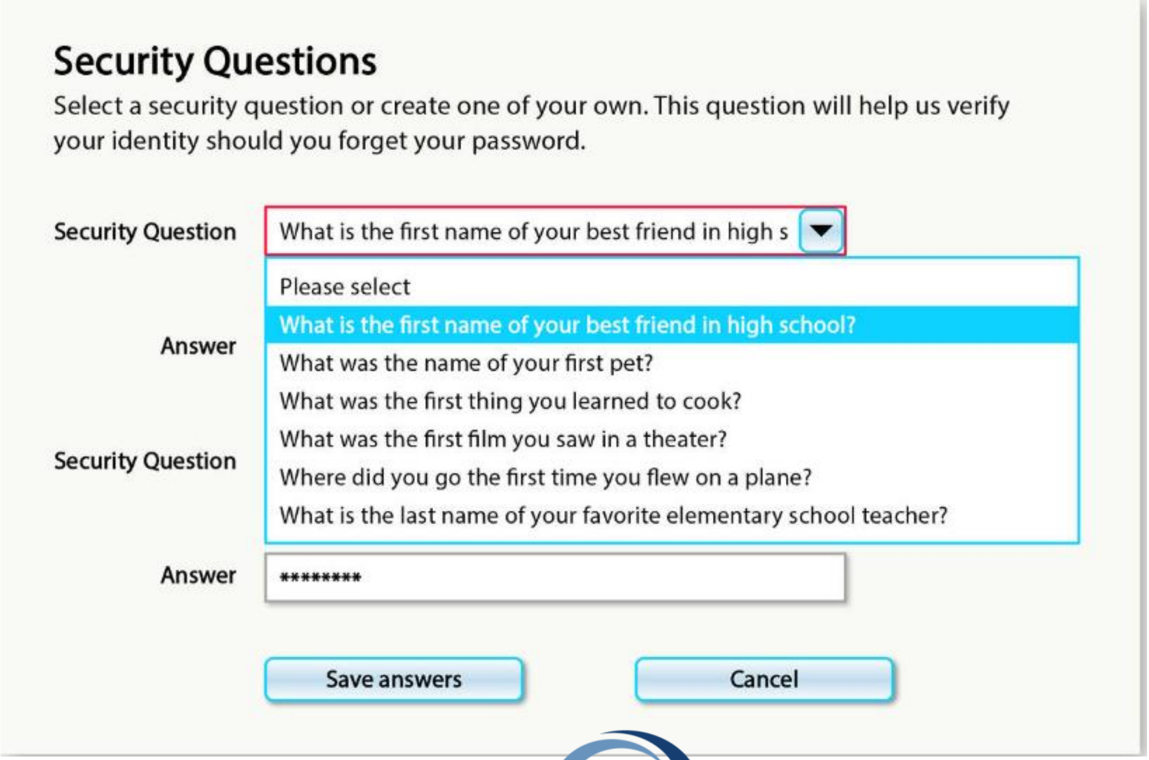
minimum 4 letters or numbers with at least one letter

Question 1: What is your pet's name?

choose an answer

Question 2

✓ What is your pet's name?
What is your favorite color?
Which street you were living when you were born?
What is your maternal grandfather's first name?
What is your favorite school teacher's name?



Security Questions

Select a security question or create one of your own. This question will help us verify your identity should you forget your password.

Security Question: What is the first name of your best friend in high s

Please select
What is the first name of your best friend in high school?
What was the name of your first pet?
What was the first thing you learned to cook?
What was the first film you saw in a theater?
Where did you go the first time you flew on a plane?
What is the last name of your favorite elementary school teacher?

Answer

Security Question

Answer: ********

VantagePoint
EMPLOYEE OWNED

Summary

Mobile devices should be respected in all they can do

Security in Layers

Proactive not reactive

“Inspect what you Expect” aka, “train, train and train some more”

THANK YOU

Further Questions?

Email to get answers:

James.taylor@vantagepnt.com

VantagePoint
EMPLOYEE OWNED