2018 Phishing Trip

Andrew Dubiel

Scott Kaylor

years of

Innovation and **Member Service**

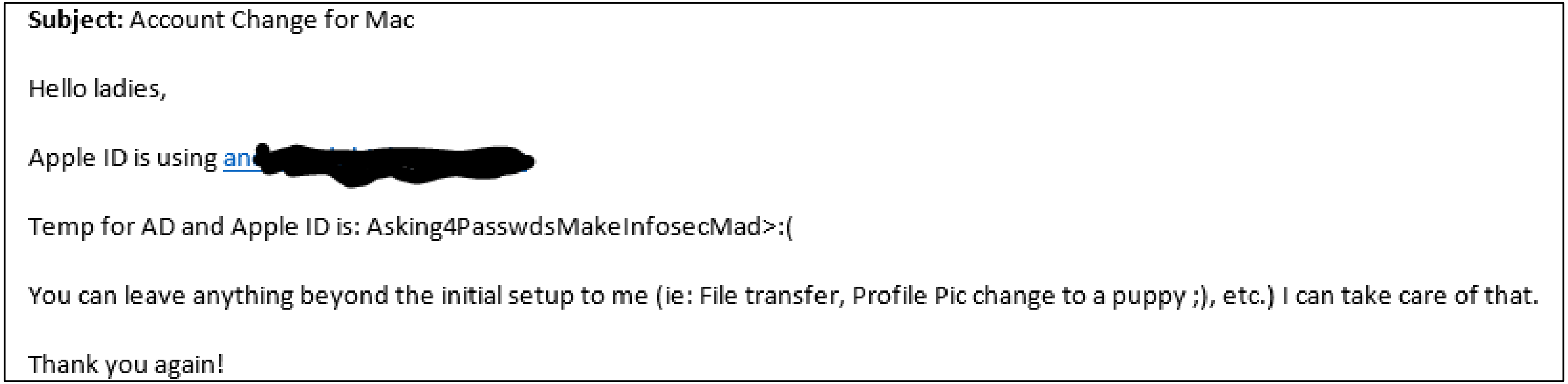
Cybersecurity Services℠

Outcomes

- Understand a password
- Know how a password is stored
- Know how to steal a password
- Identify different methods of phishing
- Tell the difference between Phishing vs. Spam
- Practical security for a company's environment
- Never trust a pretty pony again!

Why Am I Even Here?

- To prevent this!!!



Subject: Account Change for Mac

Hello ladies,

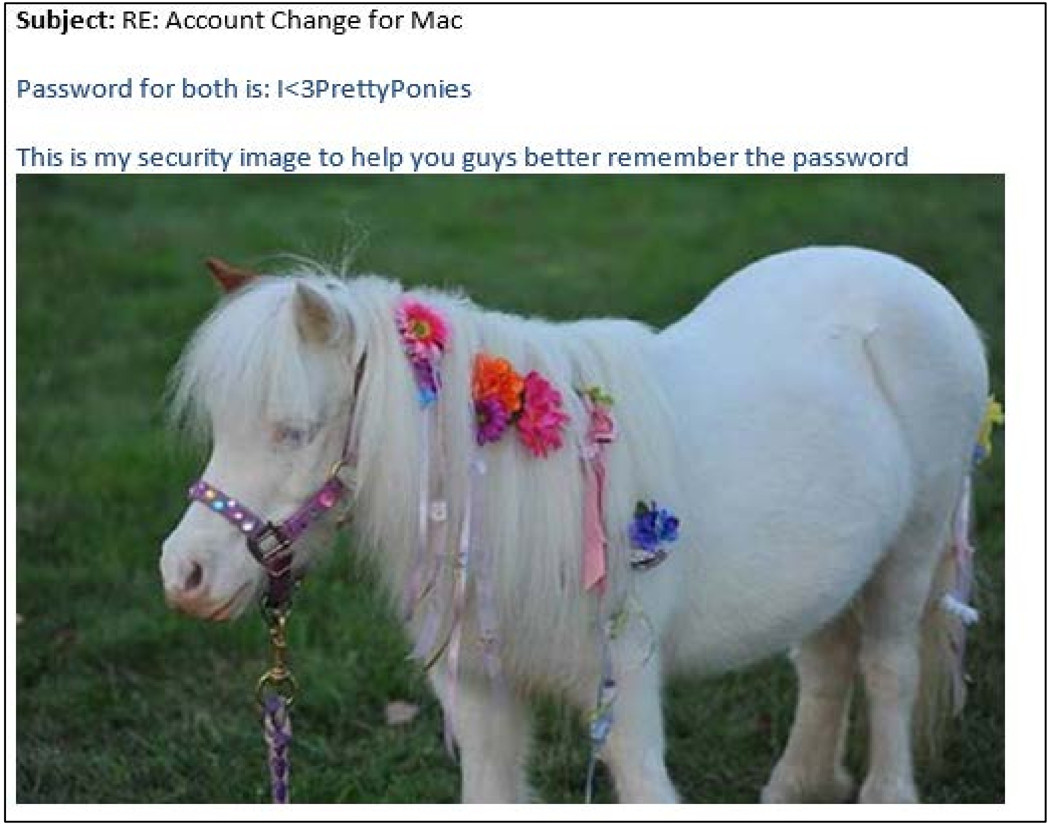
Apple ID is using [redacted]

Temp for AD and Apple ID is: Asking4PasswdsMakeInfosecMad>:(

You can leave anything beyond the initial setup to me (ie: File transfer, Profile Pic change to a puppy ;), etc.) I can take care of that.

Thank you again!

My Password was too Long… for Someone Else



Subject: RE: Account Change for Mac

Password for both is: I<3PrettyPonies

This is my security image to help you guys better remember the password

What is a password?

In General:

- It is something you know
- A collection of characters
- Passphrase, Passcode, Padlock

Moving Forward:

- 8+ characters
- Letters, Numbers, Symbols
- Typed out

How Scary is a Password?

- My Password is:

Littledragonmanshootsbigrockets12high!

- 38-characters long
- Easy to remember
- (26-lowercase x 26-uppercase x 10-numbers x 11ish symbols) ^ 38
- Roughly 1.29x10^185 possibilities

Out in the Wild

- The five-server system uses a relatively new package of virtualization software that harnesses the power of 25 AMD Radeon graphics cards. It achieves the 350 billion-guess-per-second speed when cracking password hashes generated by the NTLM cryptographic algorithm that Microsoft has included in every version of Windows since Server 2003.
- As a result, it can try an astounding 958 combinations in just 5.5 hours, enough to brute force every possible eight-character password containing upper- and lower-case letters, digits, and symbols.

https://arstechnica.com/information-technology/2012/12/25-gpu-cluster-cracks-every-standard-windows-password-in-6-hours/

A Password’s Natural Habitat

- Assuming Database is configured properly:
  - The password at rest might be SHA-256:
    - 3A59ED35E388AF4BF7AAFEDBFC1F6580D041A660087C99DA87440DF482863D42
    - Keep in mind salting, padding, etc.
  - (Should) Not available on the internet…
    - “Panerabread.com Leaks Millions of Customer Records”
      - April 02, 2018
      - https://krebsonsecurity.com/2018/04/panerabread-com-leaks-millions-of-customer-records/

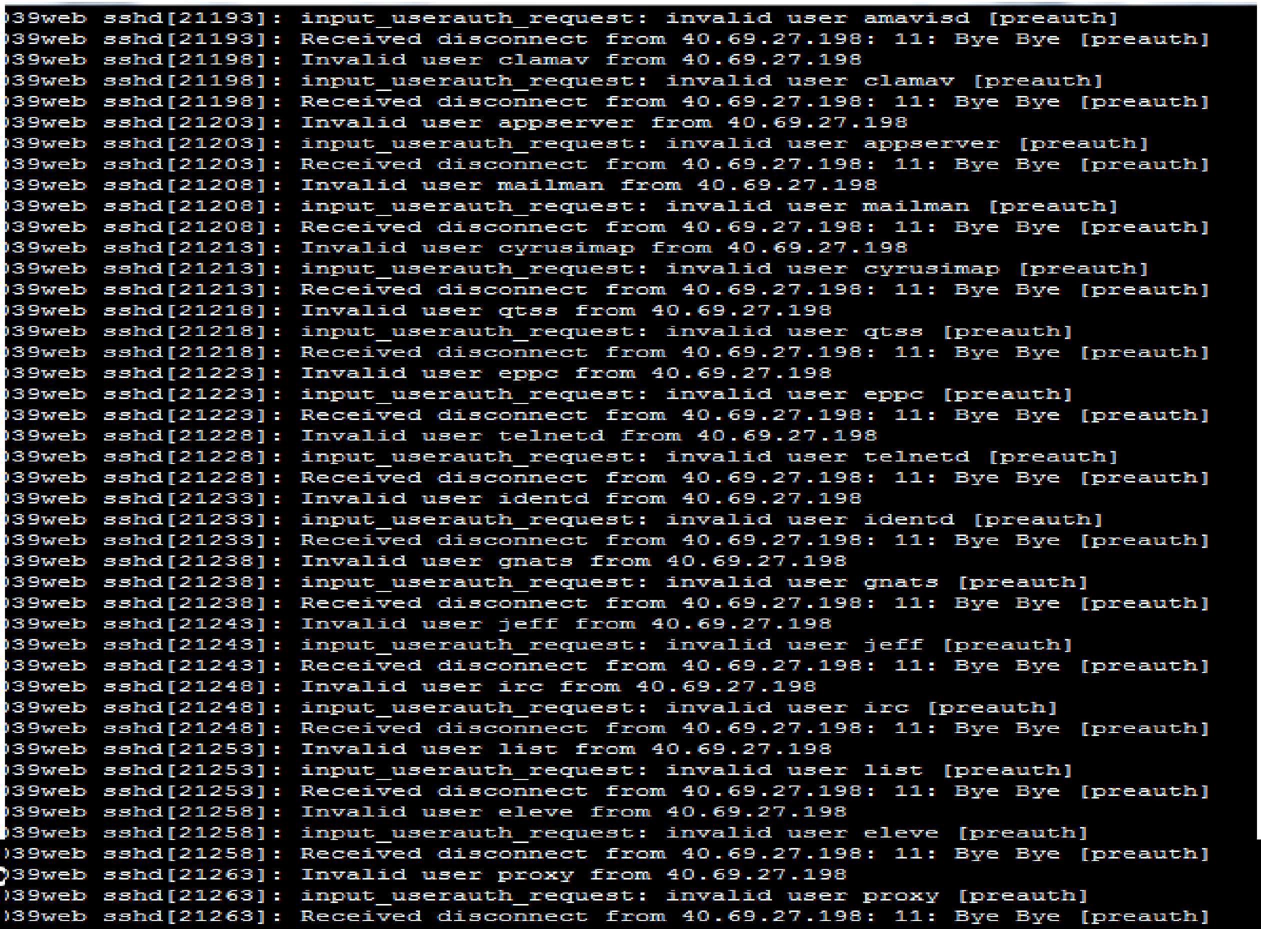
Logging into www.youtu…(del) workstuff.com

- When comparing passwords online
  - Type password into password box:
    - F22F4F20E9AA8F9EFA1B50AAA171F92EAB5F4198537DEBC8FC524513580EE2C8
      - Decrypted: “You just got rick rolled!”
  - Website then looks up user’s password in DB:
    - 0424974C68530290458C8D58674E2637F65ABC127057957D7B3ACBD24C208F93
      - Decrypted: (https://www.youtube.com/watch?v=dQw4w9WgXcQ)
  - Without exposing password to clear text, passwords are not a match
    - Denied access

Brute Force

- Trying every possible combination
- Attempted offline
  - Speed
  - No timeouts or lockouts
- Or you’re these guys…

Brute Force – Wordlist

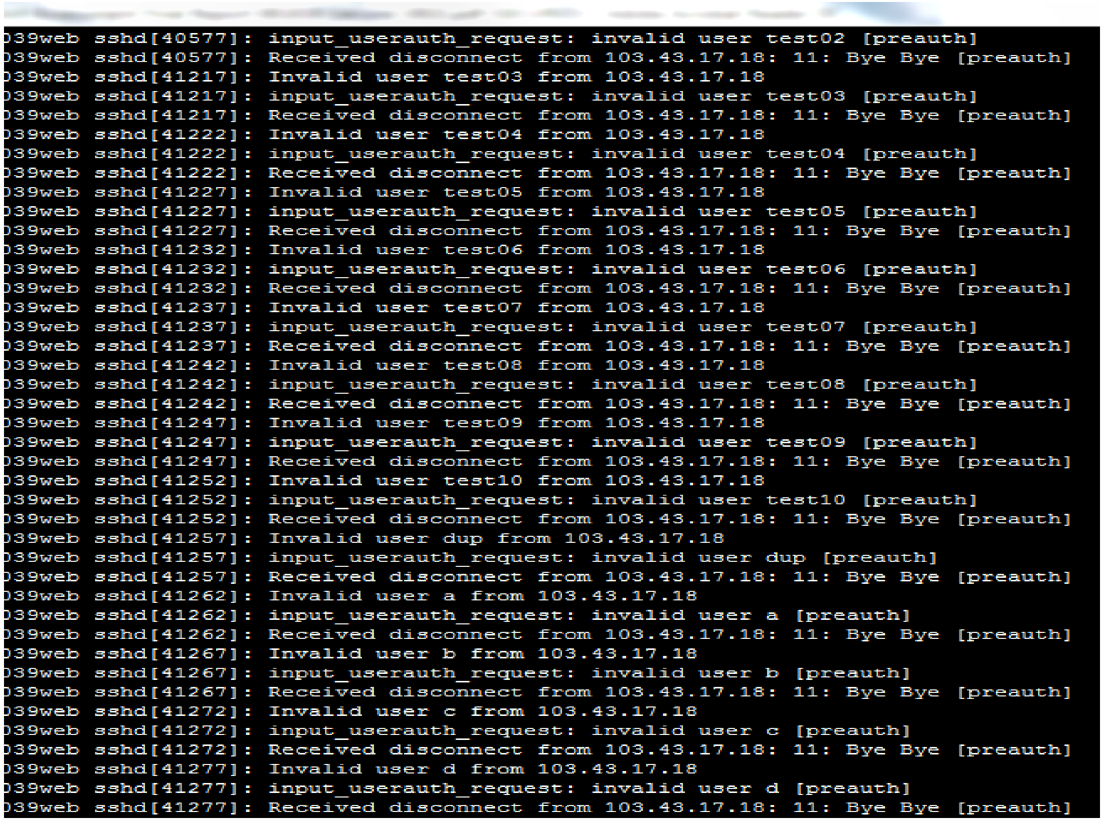


```
39web sshd[21193]: input_userauth_request: invalid user amavisd [preauth]
39web sshd[21193]: Received disconnect from 40.69.27.198: 11: Bye Bye [preauth]
39web sshd[21198]: Invalid user clamav from 40.69.27.198
39web sshd[21198]: input_userauth_request: invalid user clamav [preauth]
39web sshd[21198]: Received disconnect from 40.69.27.198: 11: Bye Bye [preauth]
39web sshd[21203]: Invalid user appserver from 40.69.27.198
39web sshd[21203]: input_userauth_request: invalid user appserver [preauth]
39web sshd[21203]: Received disconnect from 40.69.27.198: 11: Bye Bye [preauth]
39web sshd[21208]: Invalid user mailman from 40.69.27.198
39web sshd[21208]: input_userauth_request: invalid user mailman [preauth]
39web sshd[21208]: Received disconnect from 40.69.27.198: 11: Bye Bye [preauth]
39web sshd[21213]: Invalid user cyrusimap from 40.69.27.198
39web sshd[21213]: input_userauth_request: invalid user cyrusimap [preauth]
39web sshd[21213]: Received disconnect from 40.69.27.198: 11: Bye Bye [preauth]
39web sshd[21218]: Invalid user qtss from 40.69.27.198
39web sshd[21218]: input_userauth_request: invalid user qtss [preauth]
39web sshd[21218]: Received disconnect from 40.69.27.198: 11: Bye Bye [preauth]
39web sshd[21223]: Invalid user eppc from 40.69.27.198
39web sshd[21223]: input_userauth_request: invalid user eppc [preauth]
39web sshd[21223]: Received disconnect from 40.69.27.198: 11: Bye Bye [preauth]
39web sshd[21228]: Invalid user telnetd from 40.69.27.198
39web sshd[21228]: input_userauth_request: invalid user telnetd [preauth]
39web sshd[21228]: Received disconnect from 40.69.27.198: 11: Bye Bye [preauth]
39web sshd[21233]: Invalid user identd from 40.69.27.198
39web sshd[21233]: input_userauth_request: invalid user identd [preauth]
39web sshd[21233]: Received disconnect from 40.69.27.198: 11: Bye Bye [preauth]
39web sshd[21238]: Invalid user gnats from 40.69.27.198
39web sshd[21238]: input_userauth_request: invalid user gnats [preauth]
39web sshd[21238]: Received disconnect from 40.69.27.198: 11: Bye Bye [preauth]
39web sshd[21243]: Invalid user jeff from 40.69.27.198
39web sshd[21243]: input_userauth_request: invalid user jeff [preauth]
39web sshd[21243]: Received disconnect from 40.69.27.198: 11: Bye Bye [preauth]
39web sshd[21248]: Invalid user irc from 40.69.27.198
39web sshd[21248]: input_userauth_request: invalid user irc [preauth]
39web sshd[21248]: Received disconnect from 40.69.27.198: 11: Bye Bye [preauth]
39web sshd[21253]: Invalid user list from 40.69.27.198
39web sshd[21253]: input_userauth_request: invalid user list [preauth]
39web sshd[21253]: Received disconnect from 40.69.27.198: 11: Bye Bye [preauth]
39web sshd[21258]: Invalid user eleve from 40.69.27.198
39web sshd[21258]: input_userauth_request: invalid user eleve [preauth]
39web sshd[21258]: Received disconnect from 40.69.27.198: 11: Bye Bye [preauth]
39web sshd[21263]: Invalid user proxy from 40.69.27.198
39web sshd[21263]: input_userauth_request: invalid user proxy [preauth]
39web sshd[21263]: Received disconnect from 40.69.27.198: 11: Bye Bye [preauth]
```

Tried:

- clamav
- appserver
- mailman
- eppc
- telnetd
- gnats
- jeff
- list
- proxy
- eleve
- zzz
- dan
- frank
- james
- **prettypony?**

Brute Force – Plus One



```
39web sshd[40577]: input_userauth_request: invalid user test02 [preauth]
39web sshd[40577]: Received disconnect from 103.43.17.18: 11: Bye Bye [preauth]
39web sshd[41217]: Invalid user test03 from 103.43.17.18
39web sshd[41217]: input_userauth_request: invalid user test03 [preauth]
39web sshd[41217]: Received disconnect from 103.43.17.18: 11: Bye Bye [preauth]
39web sshd[41222]: Invalid user test04 from 103.43.17.18
39web sshd[41222]: input_userauth_request: invalid user test04 [preauth]
39web sshd[41222]: Received disconnect from 103.43.17.18: 11: Bye Bye [preauth]
39web sshd[41227]: Invalid user test05 from 103.43.17.18
39web sshd[41227]: input_userauth_request: invalid user test05 [preauth]
39web sshd[41227]: Received disconnect from 103.43.17.18: 11: Bye Bye [preauth]
39web sshd[41232]: Invalid user test06 from 103.43.17.18
39web sshd[41232]: input_userauth_request: invalid user test06 [preauth]
39web sshd[41232]: Received disconnect from 103.43.17.18: 11: Bye Bye [preauth]
39web sshd[41237]: Invalid user test07 from 103.43.17.18
39web sshd[41237]: input_userauth_request: invalid user test07 [preauth]
39web sshd[41237]: Received disconnect from 103.43.17.18: 11: Bye Bye [preauth]
39web sshd[41242]: Invalid user test08 from 103.43.17.18
39web sshd[41242]: input_userauth_request: invalid user test08 [preauth]
39web sshd[41242]: Received disconnect from 103.43.17.18: 11: Bye Bye [preauth]
39web sshd[41247]: Invalid user test09 from 103.43.17.18
39web sshd[41247]: input_userauth_request: invalid user test09 [preauth]
39web sshd[41247]: Received disconnect from 103.43.17.18: 11: Bye Bye [preauth]
39web sshd[41252]: Invalid user test10 from 103.43.17.18
39web sshd[41252]: input_userauth_request: invalid user test10 [preauth]
39web sshd[41252]: Received disconnect from 103.43.17.18: 11: Bye Bye [preauth]
39web sshd[41257]: Invalid user dup from 103.43.17.18
39web sshd[41257]: input_userauth_request: invalid user dup [preauth]
39web sshd[41257]: Received disconnect from 103.43.17.18: 11: Bye Bye [preauth]
39web sshd[41262]: Invalid user a from 103.43.17.18
39web sshd[41262]: input_userauth_request: invalid user a [preauth]
39web sshd[41262]: Received disconnect from 103.43.17.18: 11: Bye Bye [preauth]
39web sshd[41267]: Invalid user b from 103.43.17.18
39web sshd[41267]: input_userauth_request: invalid user b [preauth]
39web sshd[41267]: Received disconnect from 103.43.17.18: 11: Bye Bye [preauth]
39web sshd[41272]: Invalid user c from 103.43.17.18
39web sshd[41272]: input_userauth_request: invalid user c [preauth]
39web sshd[41272]: Received disconnect from 103.43.17.18: 11: Bye Bye [preauth]
39web sshd[41277]: Invalid user d from 103.43.17.18
39web sshd[41277]: input_userauth_request: invalid user d [preauth]
39web sshd[41277]: Received disconnect from 103.43.17.18: 11: Bye Bye [preauth]
```

Tried:

- test02
- test03
- test04
- …
- a
- b
- c
- d

DIY – Password Stealing

- Things you will need:
  - User Account
  - The correct system
  - Hashing algorithm used
    - PBKDF2, bcrypt or scrypt, MD-5, SHA-256, proprietary?
    - Salt: a non-secret, unique value in the database which is appended (depending on the used algorithm) to the password before it gets hashed.
    - Pepper: a secret value (a key) which is used to turn the hash into a HMAC.
  - Fire Power
    - GPUs, GPUs, GPUs, GPUs
  - *optional* Database
  - *optional* Private Billion Dollar Botnet Farm
  - *optional* One Password Granting Pretty Pony

DIY – Password Security

- Things you will need:
  - Company Password Policy
    - Min, Max, Rotation, Etc.
  - Enforcement / Testing
    - Test Active Directory Passwords
  - Password Hygiene
    - Never write down, disclose, etc.
    - If you do, NEVER have identifying items together
  - Complexity in length, not memorization
    - 5Brownmoons1n5months$ vs. 592TTg$$
    - NISC - “Did you crack my password? It’s not found in a dictionary!! It’s 7 characters.”

Phishing – Because password cracking is hard

- In General
  - Social Engineering
  - Voice Phishing (Vishing)
  - SMS Phishing
  - Evil Twin (WiFi)
  - Whaling
  - Spear Phishing
  - Link Manipulation

- Moving Forward
  - Spear Phishing
  - Emails

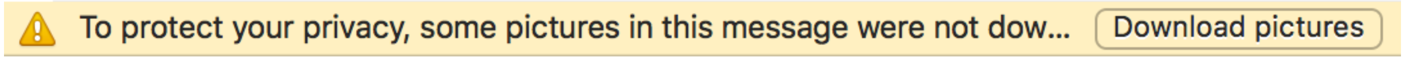
Spam vs. Phishing

- Phishing is an art
- Spam is a generic blanket
- Phishing is personal
- Spam is generally very naughty

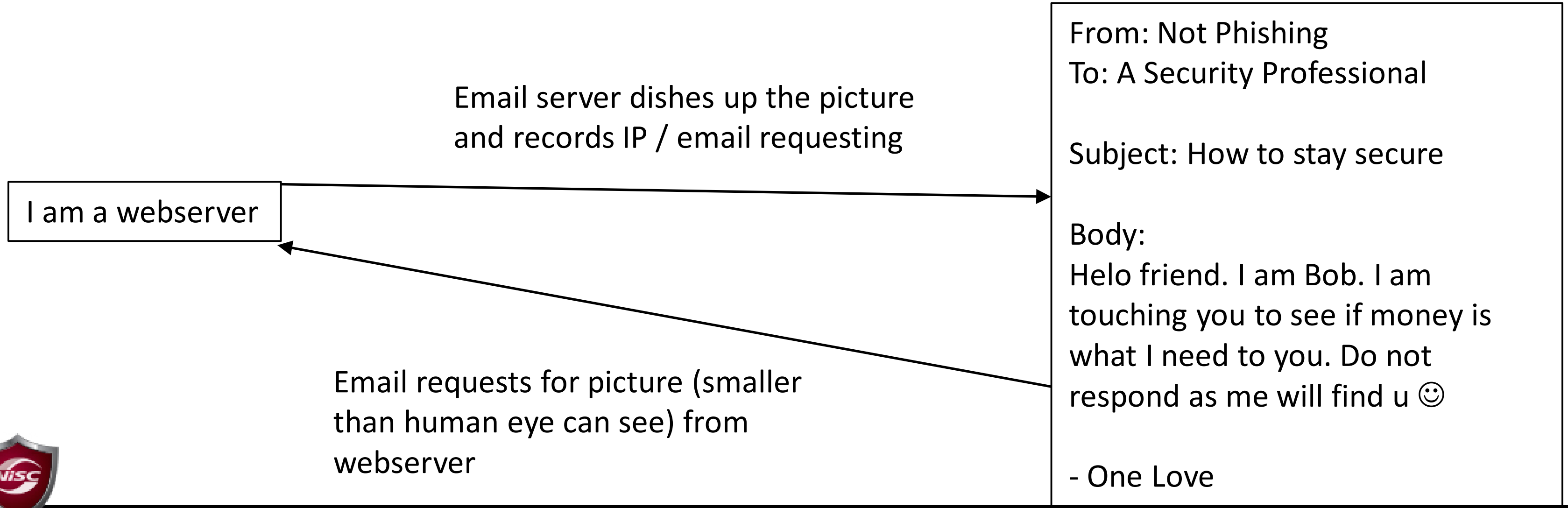
- 99% of the time, Phishing is requesting user interaction
  - Click here
  - Go here
  - Call here

The other 1%

- Emails used for tracking
  - "Active" emails are then phished in the future



⚠ To protect your privacy, some pictures in this message were not dow...



Email server dishes up the picture and records IP / email requesting

I am a webserver

Email requests for picture (smaller than human eye can see) from webserver

From: Not Phishing
To: A Security Professional

Subject: How to stay secure

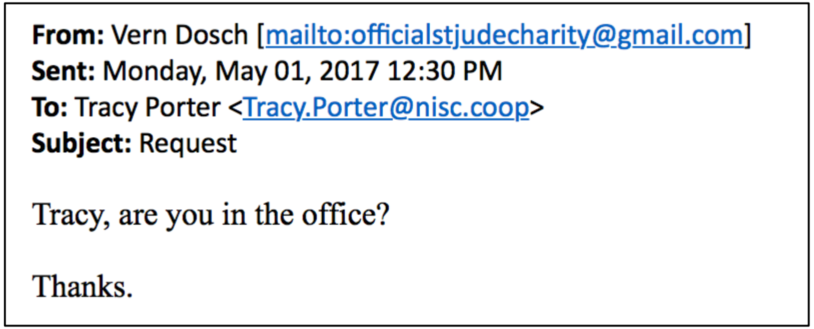
Body:
Helo friend. I am Bob. I am touching you to see if money is what I need to you. Do not respond as me will find u ☺

- One Love

Spoofed Emails

- Appear more convincing
- Piece together information from Facebook, website, conferences, etc.
- Easy enough to do (For a Cyber Criminal)

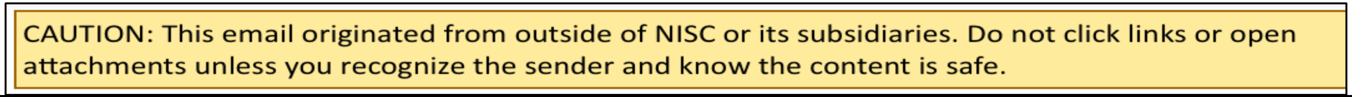
- Take Note:
  - From Address
  - Look at email headers
  - A request for interaction
    - In this case a reply



From: Vern Dosch [mailto:officialstjudecharity@gmail.com]
Sent: Monday, May 01, 2017 12:30 PM
To: Tracy Porter <Tracy.Porter@nisc.coop>
Subject: Request

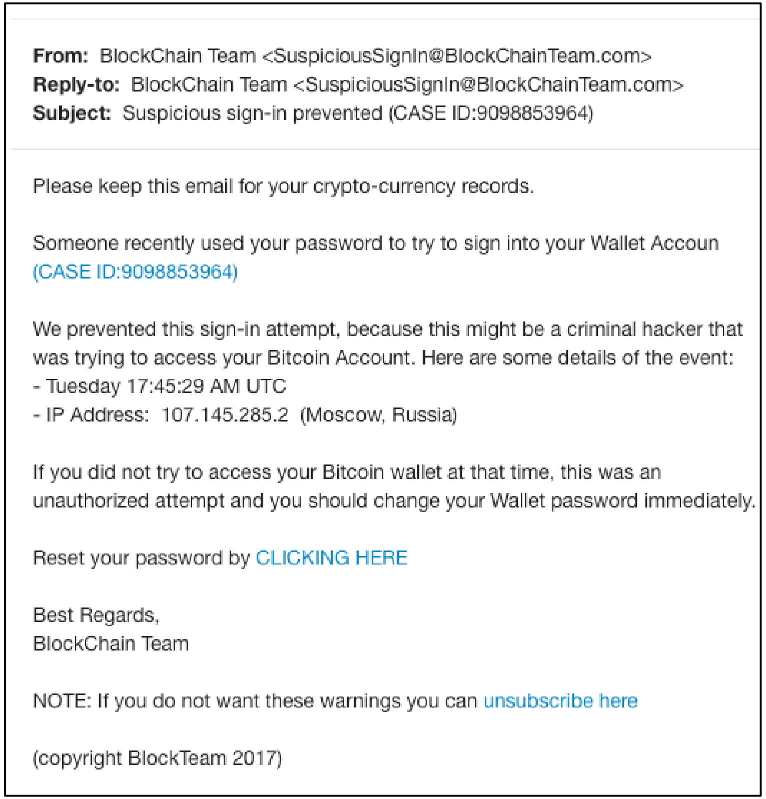
Tracy, are you in the office?

Thanks.



CAUTION: This email originated from outside of NISC or its subsidiaries. Do not click links or open attachments unless you recognize the sender and know the content is safe.

Lets Review



From: BlockChain Team <SuspiciousSignIn@BlockChainTeam.com>
Reply-to: BlockChain Team <SuspiciousSignIn@BlockChainTeam.com>
Subject: Suspicious sign-in prevented (CASE ID:9098853964)

Please keep this email for your crypto-currency records.

Someone recently used your password to try to sign into your Wallet Accoun (CASE ID:9098853964)

We prevented this sign-in attempt, because this might be a criminal hacker that was trying to access your Bitcoin Account. Here are some details of the event:
- Tuesday 17:45:29 AM UTC
- IP Address: 107.145.285.2 (Moscow, Russia)

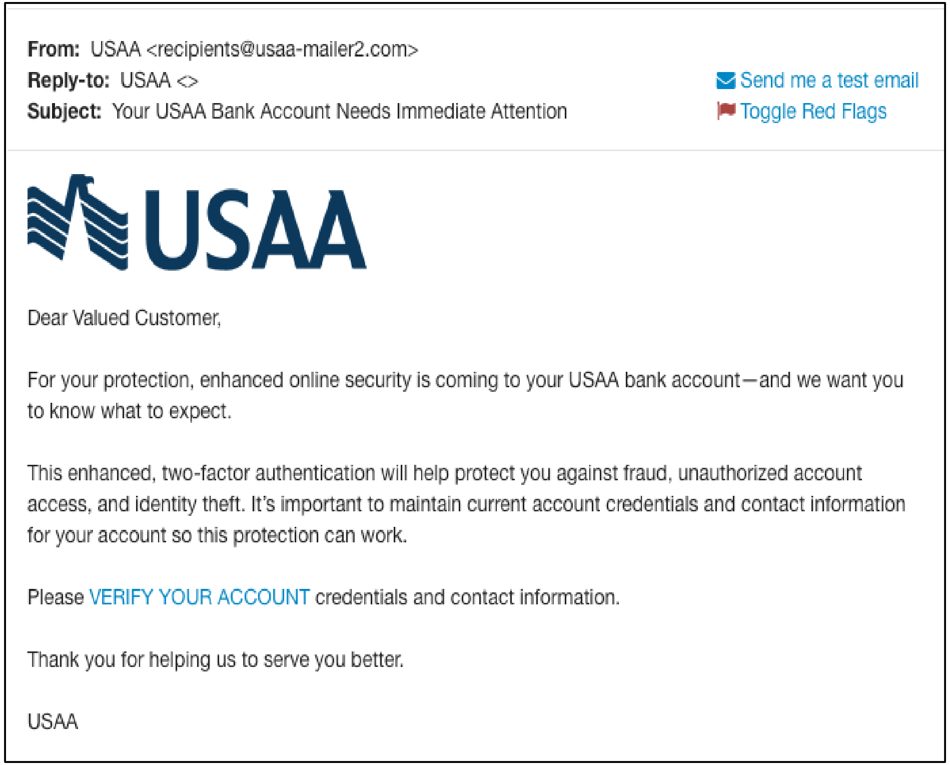
If you did not try to access your Bitcoin wallet at that time, this was an unauthorized attempt and you should change your Wallet password immediately.

Reset your password by CLICKING HERE

Best Regards,
BlockChain Team

NOTE: If you do not want these warnings you can unsubscribe here

(copyright BlockTeam 2017)



From: USAA <recipients@usaa-mailer2.com>
Reply-to: USAA <>
Subject: Your USAA Bank Account Needs Immediate Attention

Dear Valued Customer,

For your protection, enhanced online security is coming to your USAA bank account—and we want you to know what to expect.

This enhanced, two-factor authentication will help protect you against fraud, unauthorized account access, and identity theft. It's important to maintain current account credentials and contact information for your account so this protection can work.

Please VERIFY YOUR ACCOUNT credentials and contact information.

Thank you for helping us to serve you better.

USAA

DIY – Phishing

- What you will need:
  - Targets
  - Company Information (Website, emails, Org Structure, City, State, etc.)
  - Personal Information (Facebook, Twitter, Names, Locations, Banks Used, etc.)
  - Email server
    - *Optional* Hack an email server and make it your own email server
  - Spell Check
  - Persistence

DIY – Email Security

- Things you will need:
  - SECURITY AWARENESS / CULTURE

DIY – Email Security Extras

- Things you will need:
  - *SECURITY AWARENESS / CULTURE*!!!!!!!!!!!!!!!!!!!!!
  - Employees are the best line of defense!
  - Invest in employees before $1,000,000 in IT Security "Silver Bullets"

DIY – Email Security Extra Extras

- Things you will need:
  - Secure email server (Update, Patch, Update again, Patch more)
  - Secure firewall
    - An email might hit a users inbox, but a firewall will block malicious traffic
  - Testing / Reporting Solutions (KnowBe4, Rapid7 InsightPhish, etc.)
  - “Think before you click” email banners (IP / domain based)
  - Whitelist on email server
  - Log monitoring
    - Rapid7 caught O365 authentications from different states
  - Two factor authentication (Word of the day)

Creating a Security Culture

- Allow / encourage questions
  - No question is a dumb question
- Win or Lose – Employees determine company's fate
- Lock computers
- Password hygiene
  - Lastpass vs. Paper and Pen
- Consistency
  - Outlook vs. Gmail vs. Dropbox vs. iCloud
- Teach, test, reinforce

Questions?

Remember…

Pretty ponies belong on a farm, not a business!!

Thank You!