Reducing the Risk of a Cyber Attack in Higher Education

WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING

Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor

Disclaimer

The information contained herein is general in nature and is not intended, and should not be construed, as legal, accounting, or tax advice or opinion provided by CliftonLarsonAllen LLP to the user. The user also is cautioned that this material may not be applicable to, or suitable for, the user's specific circumstances or needs, and may require consideration of non-tax and other tax factors if any action is to be contemplated. The user should contact his or her CliftonLarsonAllen LLP or other tax professional prior to taking any action based upon this information. CliftonLarsonAllen LLP assumes no obligation to inform the user of any changes in tax laws or other factors that could affect the information contained herein.

IT & Cyber Security Services

Information Security offered as specialized service offering for over 25 years

- Penetration Testing and Vulnerability Assessment
    - Black Box, Red Team, Infrastructure, Applications, Social Engineering, and Collaborative Assessments
- Incident response and forensics
- IT/Cyber risk, audit, readiness and compliance assessments
    - HIPAA, GLBA, FFIEC, NIST, CMMC, CIS, etc…
- PCI-DSS Readiness and Compliance Assessments
- HITRUST Assessments
- SOC Assessment and Reporting
- Business Risk Services
- Digital Transformation

Our Panelists

Kadian Douglas	David Anderson	Zoran Jovic
Principal, Cybersecurity	Principal, Cybersecurity	Senior, Cybersecurity
Kadian.Douglas@CLAconnect.com	David.Anderson@CLAconnect.com	Zoran.Jovic@CLAconnect.com
813-384-2735	612-376-4699	813-384-2728

Agenda and Learning Objectives

Agenda

- Current Cybersecurity Trends
- Email Phishing and Credential Compromise
- Managing the Risk

Learning Objectives

- Identify key risk factors surrounding today’s cyber threat landscape
- Recognize how attackers plan and execute attacks such as phishing and password guessing
- Identify how to better defend yourself and your institution from becoming a victim of a cyberattack
- Recognize key strategies in creating secure passwords and improving overall security

Polling Question 1:

Do currently have a documented risk assessment or information security program?

a. Information Security Program
b. Risk Assessment
c. Both
d. Neither

Current Cybersecurity Landscape

WEALTH ADVISORY | OUTSOURCING
AUDIT, TAX, AND CONSULTING

Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor

Cybersecurity Landscape in 2021

- As a result of the pandemic, we have seen both traditional, and more commonly, nontraditional forms of hacking targeting all Industry sectors.

- COVID and the remote working transition continues to present challenges with most organization’s cyber security strategy.

- Remote learning increases the ”attack surface” as more resources are exposed online.

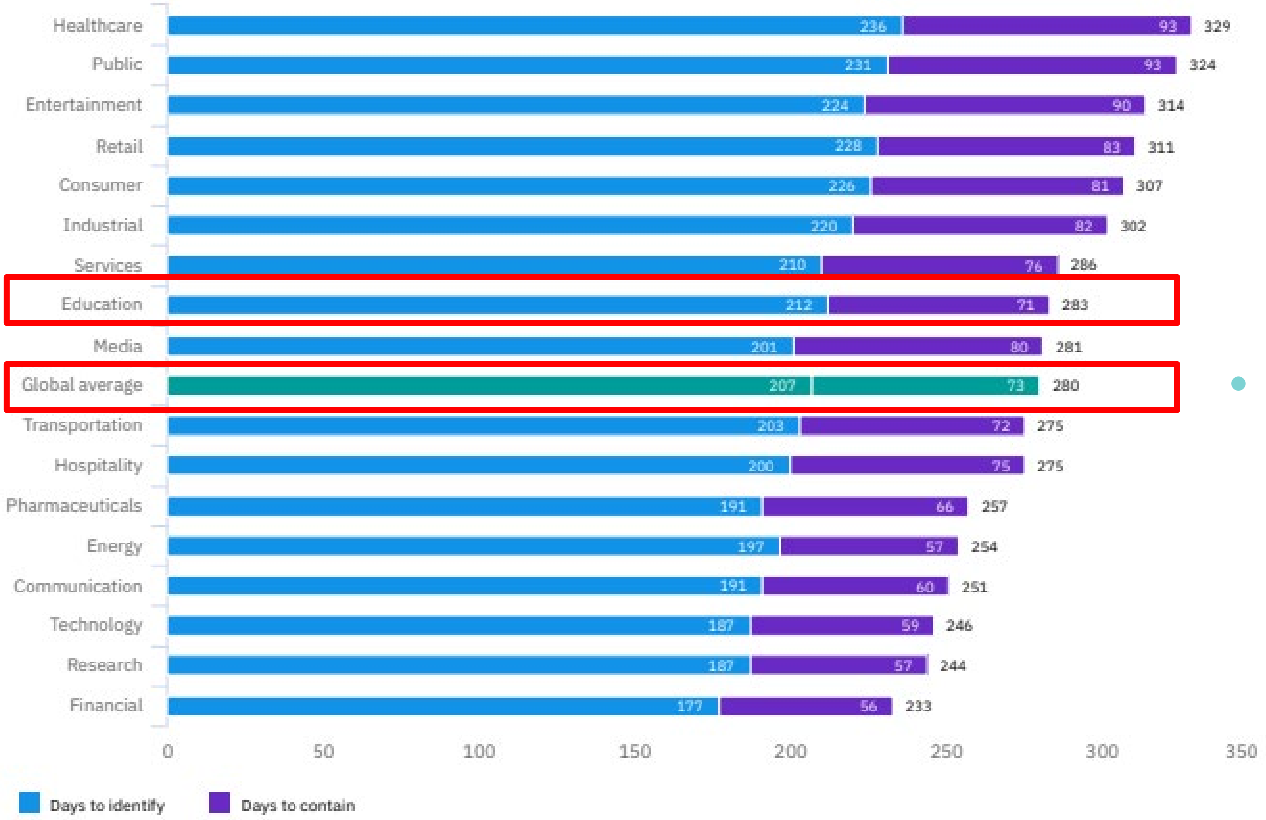
Cybersecurity – What we learned in 2020

- As organizations continued to digitize and connect, they created an ecosystem that requires a security architecture adequate to protect beyond its physical buildings.
- A robust Information Governance Strategy is a key imperative – identify and protect your Crown Jewels, and purge unneeded information.
- Leadership needs to be aware of and manage its supply chain and vendors (Vendor Risk Management). A proactive Vendor Risk Management strategy is critical to minimizing the disruption of a companies supply chain.
- Organizations must educate and inform your board of directors and senior executives. You are an important advocate in funding your cybersecurity strategy.

Cybersecurity Data Breach- Cost by the numbers

- IBM’s 2021 Cost of a Data Breach study conducted by the Ponemon Institute noted:
  - ○ **$3.79m Average cost of a data breach in the Higher Education**
  - ○ $5.33m Global average cost of breach enterprises > 25,000 employees
  - ○ $2.98m Global average cost of breach organizations < 500 employees
  - ○ +$1.07m Cost where remote workforce was a factor in causing the breach
  - ○ 44% Breaches that included records containing Customer PII
    - ➢ Average cost of $180 per record
  - ○ 38% Portion of breach costs due to lost business

Average Days to Identify and Contain a Data Breach

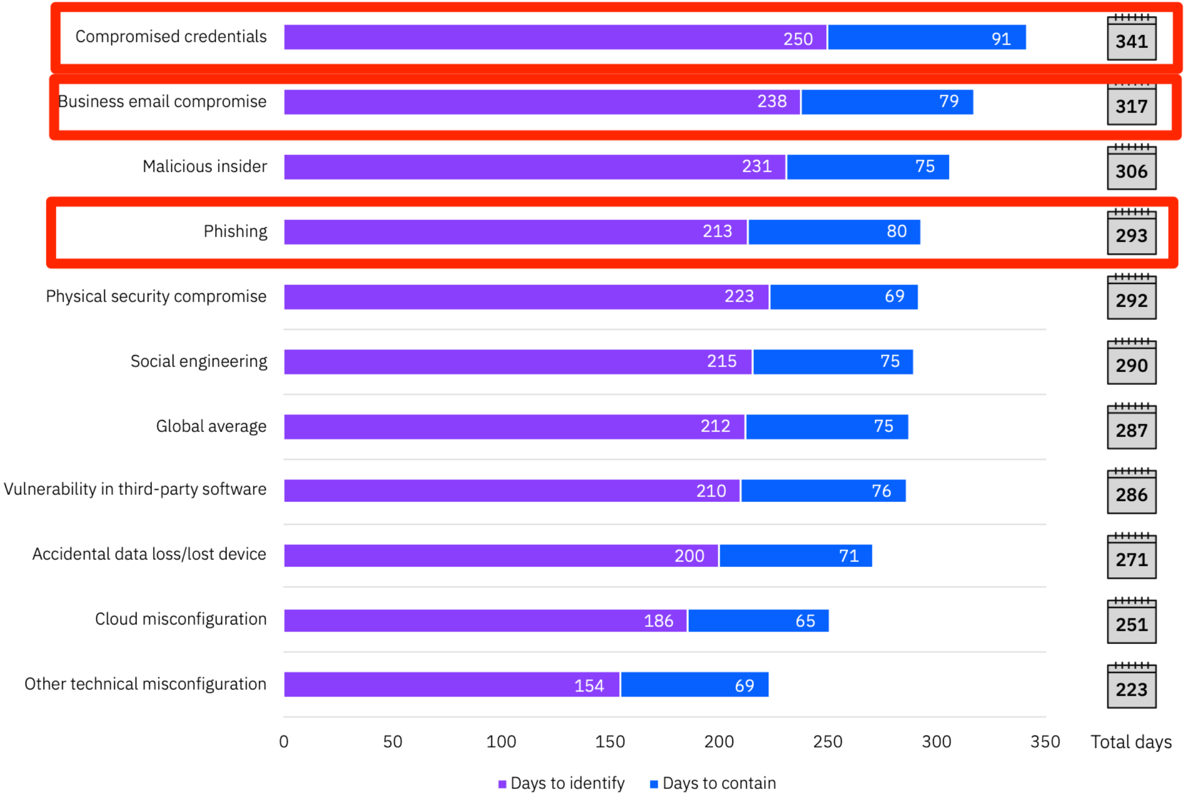


- Global average is 280 days
  - 207 days to identify a breach
  - 73 days to contain the attack

Source: IBM Security Cost of a Data Breach Report 2021

Source: IBM Security Cost of a Data Breach Report 2020

How Long Does it Take to Identify and Contain?



Source: IBM Security Cost of a Data Breach Report 2021

Social Engineering – Email Phishing

WEALTH ADVISORY | OUTSOURCING
AUDIT, TAX, AND CONSULTING

Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor

Social Engineering in Higher Education?

- Risk Factors:
  - Constantly changing “client base”
  - Access to financial information
  - Access to personally identifiable information
  - Multitude of scams
  - Public reporting requirements
  - Regulatory and compliance mandates

Social Engineering

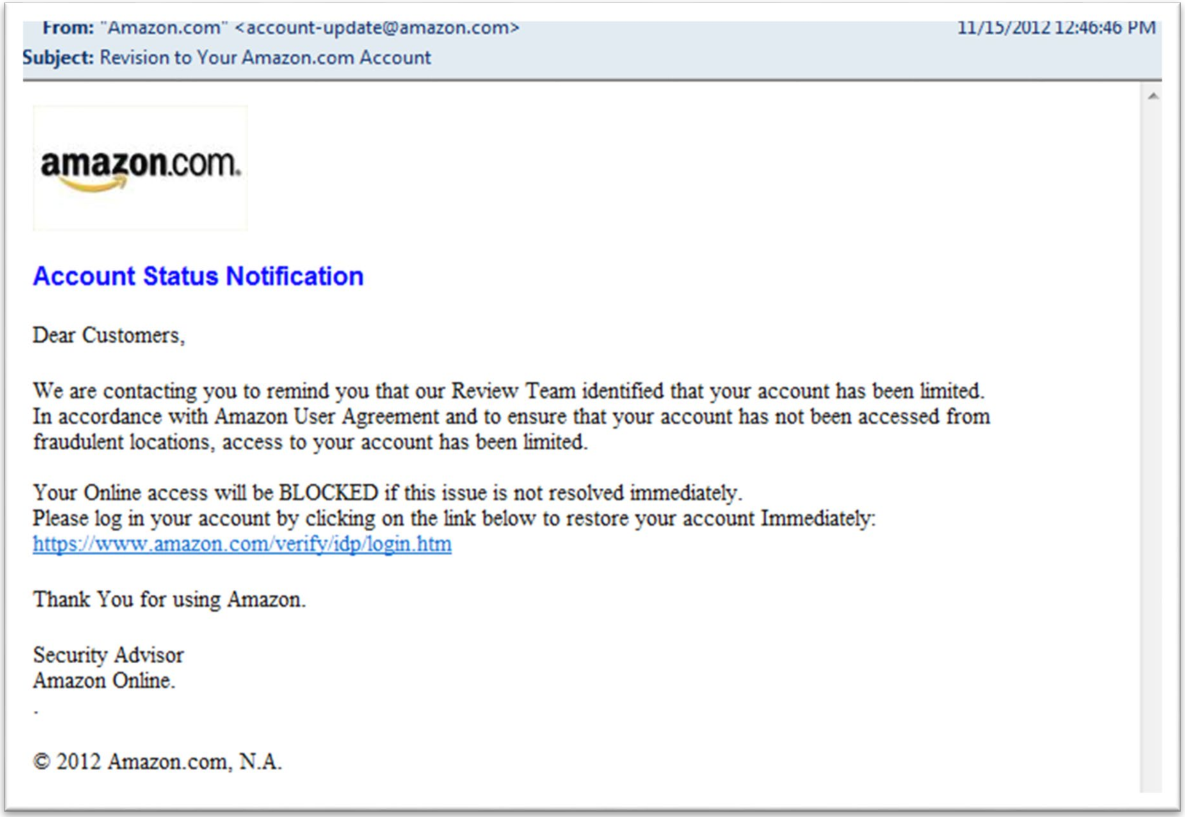
- Hacking the human
  - Simply put, Social Engineering is the exploitation of human nature
  - Psychological manipulation of people into performing actions or divulging confidential information
    - Pre-text Calls
    - Email Phishing
    - Manipulation of Physical Security

- Highest risk for these attacks?
  - New employees/New Students
  - Contractors – third parties
  - Executive assistants
  - “Multitaskers”

It all starts with Information Gathering

- The ***information gathering*** process is critical. The internet can provide a host of information essential to performing a successful social engineering attack
- Google images
  - Facility access, entrances
  - Type of access control used
  - Employee information
- Social Media
- Previous Breaches
- Information is a dangerous weapon. Adds legitimacy where there is none

Spotting a Malicious Link



From: "Amazon.com" <account-update@amazon.com> 11/15/2012 12:46:46 PM

Subject: Revision to Your Amazon.com Account

Account Status Notification

Dear Customers,

We are contacting you to remind you that our Review Team identified that your account has been limited. In accordance with Amazon User Agreement and to ensure that your account has not been accessed from fraudulent locations, access to your account has been limited.

Your Online access will be BLOCKED if this issue is not resolved immediately.
Please log in your account by clicking on the link below to restore your account Immediately:
https://www.amazon.com/verify/idp/login.htm

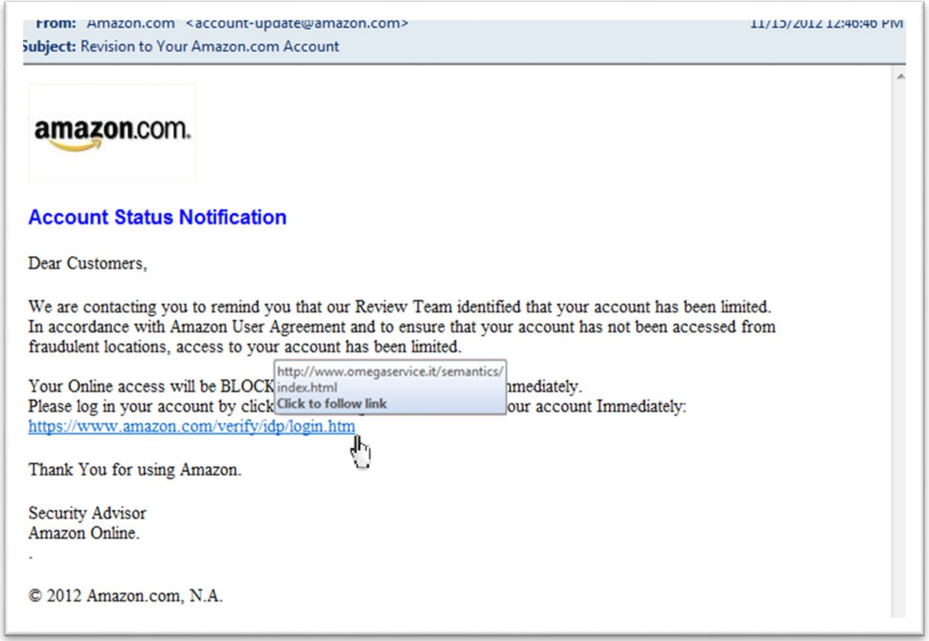
Thank You for using Amazon.

Security Advisor
Amazon Online.
.

© 2012 Amazon.com, N.A.

Uncovering a Malicious Link

- Hovering over a link with your mouse will show the true path of the link.



From: "Amazon.com" <account-update@amazon.com> 11/15/2012 12:46:46 PM

Subject: Revision to Your Amazon.com Account

Account Status Notification

Dear Customers,

We are contacting you to remind you that our Review Team identified that your account has been limited. In accordance with Amazon User Agreement and to ensure that your account has not been accessed from fraudulent locations, access to your account has been limited.

http://www.omegaservice.it/semantics/index.html
Click to follow link

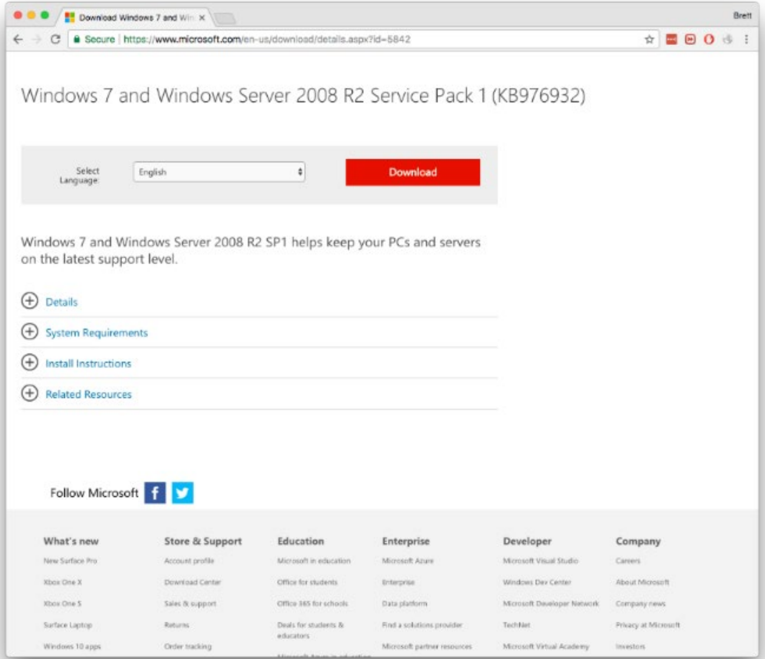
Your Online access will be BLOCK mediately.
Please log in your account by click our account Immediately:
https://www.amazon.com/verify/idp/login.htm

Thank You for using Amazon.

Security Advisor
Amazon Online.
.

© 2012 Amazon.com, N.A.

Fake vs. Real


Download Windows 7 and Win
Brett
Secure https://www.microsoft.com/en-us/download/details.aspx?id=5842

Windows 7 and Windows Server 2008 R2 Service Pack 1 (KB976932)

Select Language: English

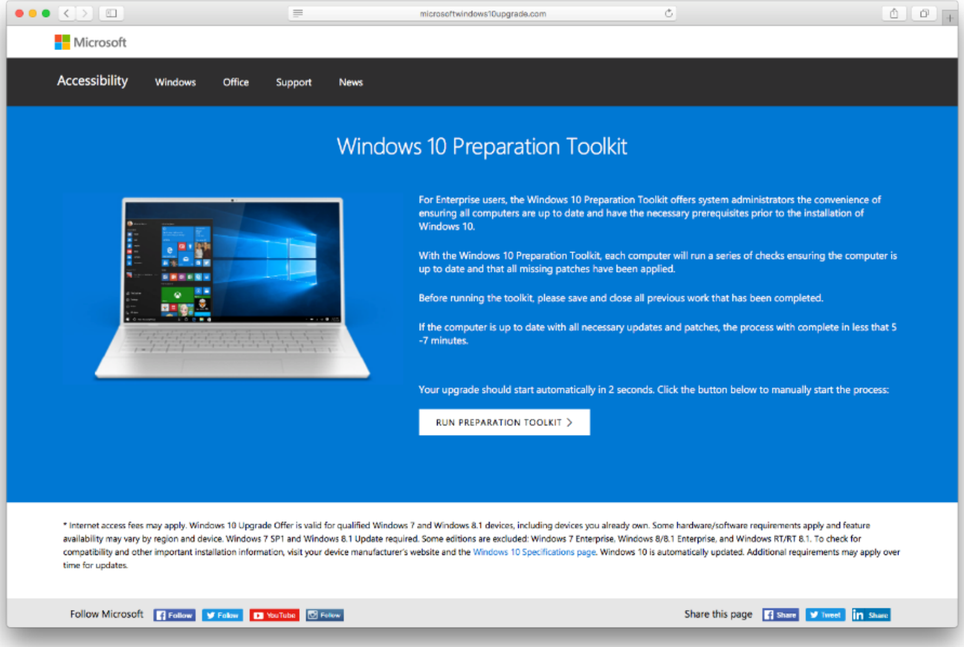
Download

Windows 7 and Windows Server 2008 R2 SP1 helps keep your PCs and servers on the latest support level.

- Details
- System Requirements
- Install Instructions
- Related Resources

Follow Microsoft

What's new	Store & Support	Education	Enterprise	Developer	Company
New Surface Pro	Account profile	Microsoft in education	Microsoft Azure	Microsoft Visual Studio	Careers
Xbox One X	Download Center	Office for students	Enterprise	Windows Dev Center	About Microsoft
Xbox One S	Sales & support	Office 365 for schools	Data platform	Microsoft Developer Network	Company news
Surface Laptop	Returns	Deals for students & educators	Find a solutions provider	TechNet	Privacy at Microsoft
Windows 10 apps	Order tracking	Microsoft Azure in education	Microsoft partner resources	Microsoft Virtual Academy	Investors



Windows 10 Preparation Toolkit

For Enterprise users, the Windows 10 Preparation Toolkit offers system administrators the convenience of ensuring all computers are up to date and have the necessary prerequisites prior to the installation of Windows 10.

With the Windows 10 Preparation Toolkit, each computer will run a series of checks ensuring the computer is up to date and that all missing patches have been applied.

Before running the toolkit, please save and close all previous work that has been completed.

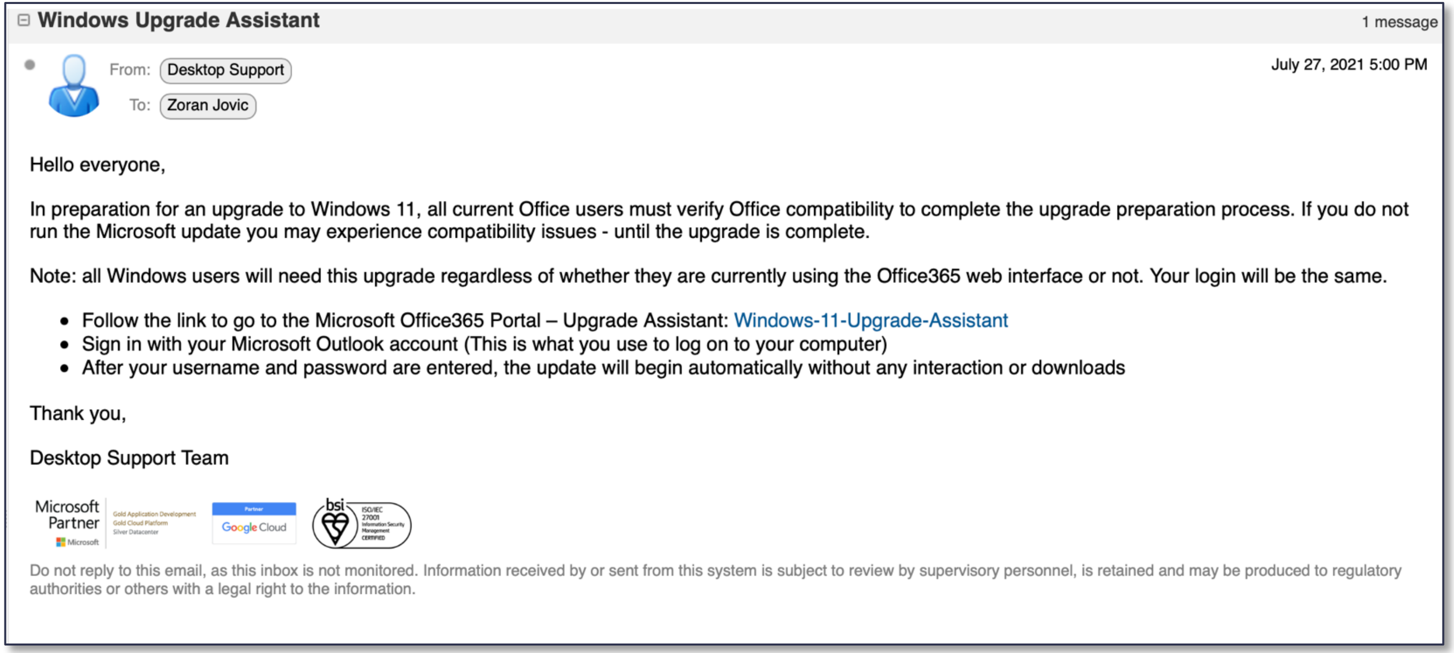
If the computer is up to date with all necessary updates and patches, the process with complete in less that 5 -7 minutes.

Your upgrade should start automatically in 2 seconds. Click the button below to manually start the process:

RUN PREPARATION TOOLKIT >

* Internet access fees may apply. Windows 10 Upgrade Offer is valid for qualified Windows 7 and Windows 8.1 devices, including devices you already own. Some hardware/software requirements apply and feature availability may vary by region and device. Windows 7 SP1 and Windows 8.1 Update required. Some editions are excluded: Windows 7 Enterprise, Windows 8/8.1 Enterprise, and Windows RT/RT 8.1. To check for compatibility and other important installation information, visit your device manufacturer's website and the Windows 10 Specifications page. Windows 10 is automatically updated. Additional requirements may apply over time for updates.

Simple Phishing Email



⊟ **Windows Upgrade Assistant**

1 message

From: Desktop Support

To: Zoran Jovic

July 27, 2021 5:00 PM

Hello everyone,

In preparation for an upgrade to Windows 11, all current Office users must verify Office compatibility to complete the upgrade preparation process. If you do not run the Microsoft update you may experience compatibility issues - until the upgrade is complete.

Note: all Windows users will need this upgrade regardless of whether they are currently using the Office365 web interface or not. Your login will be the same.

- Follow the link to go to the Microsoft Office365 Portal – Upgrade Assistant: Windows-11-Upgrade-Assistant
- Sign in with your Microsoft Outlook account (This is what you use to log on to your computer)
- After your username and password are entered, the update will begin automatically without any interaction or downloads

Thank you,

Desktop Support Team

Microsoft Partner
Microsoft

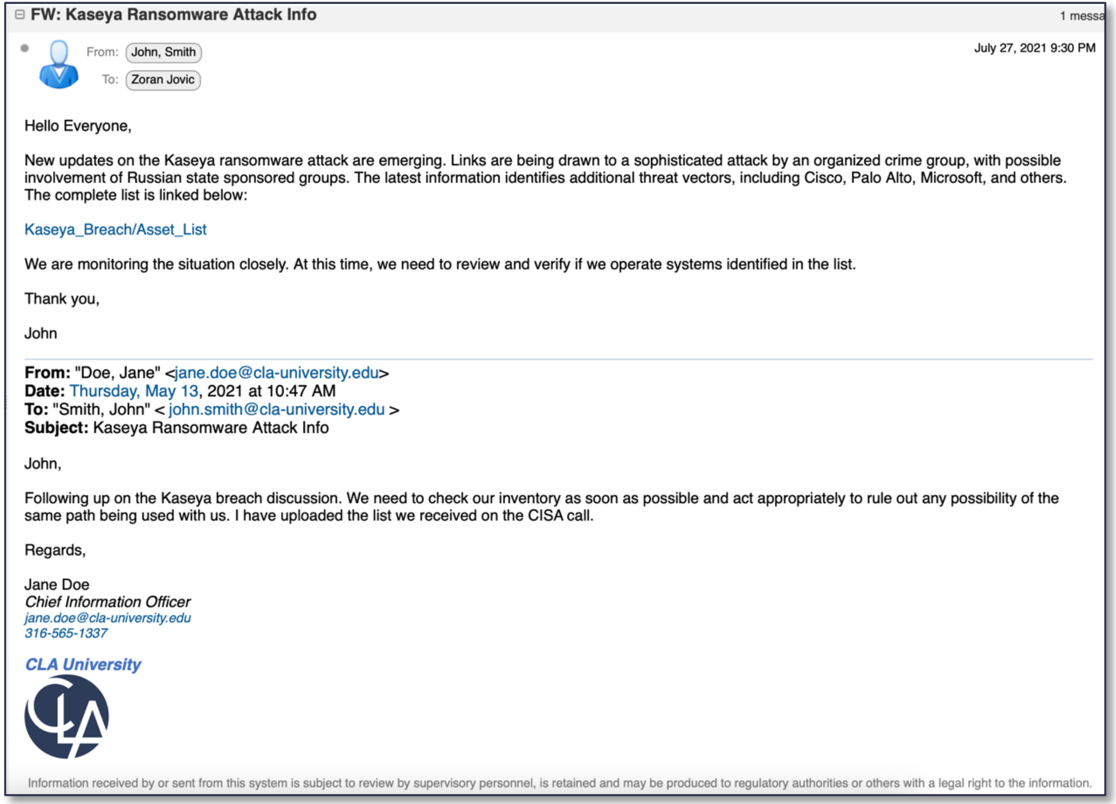
Gold Application Development
Gold Cloud Platform
Silver Datacenter

Partner
Google Cloud

bsi
ISO/IEC 27001 Information Security Management CERTIFIED

Do not reply to this email, as this inbox is not monitored. Information received by or sent from this system is subject to review by supervisory personnel, is retained and may be produced to regulatory authorities or others with a legal right to the information.

Advanced Phishing Email



⊟ **FW: Kaseya Ransomware Attack Info**

From: John, Smith

To: Zoran Jovic

July 27, 2021 9:30 PM

Hello Everyone,

New updates on the Kaseya ransomware attack are emerging. Links are being drawn to a sophisticated attack by an organized crime group, with possible involvement of Russian state sponsored groups. The latest information identifies additional threat vectors, including Cisco, Palo Alto, Microsoft, and others. The complete list is linked below:

Kaseya_Breach/Asset_List

We are monitoring the situation closely. At this time, we need to review and verify if we operate systems identified in the list.

Thank you,

John

From: "Doe, Jane" <jane.doe@cla-university.edu>
Date: Thursday, May 13, 2021 at 10:47 AM
To: "Smith, John" < john.smith@cla-university.edu >
Subject: Kaseya Ransomware Attack Info

John,

Following up on the Kaseya breach discussion. We need to check our inventory as soon as possible and act appropriately to rule out any possibility of the same path being used with us. I have uploaded the list we received on the CISA call.

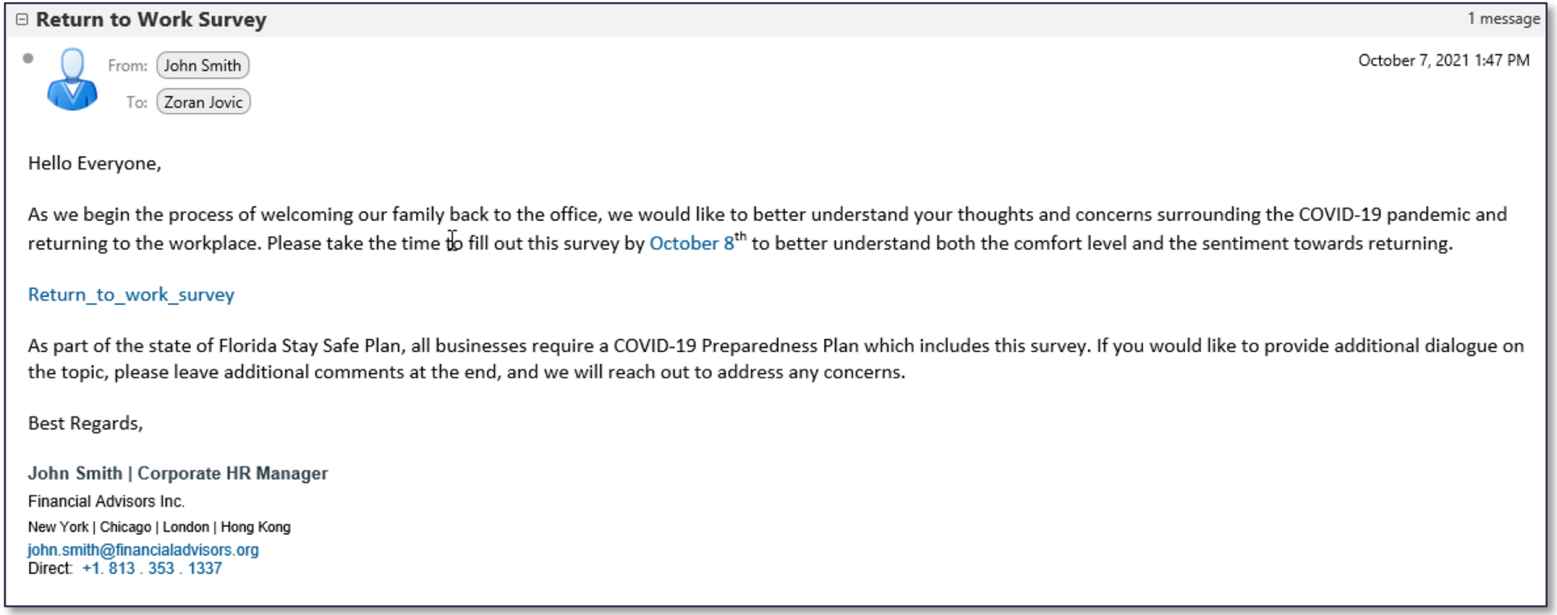
Regards,

Jane Doe
Chief Information Officer
jane.doe@cla-university.edu
316-565-1337

CLA University

Information received by or sent from this system is subject to review by supervisory personnel, is retained and may be produced to regulatory authorities or others with a legal right to the information.

Unfair Phishing Email



⊟ **Return to Work Survey**

1 message

From: John Smith

To: Zoran Jovic

October 7, 2021 1:47 PM

Hello Everyone,

As we begin the process of welcoming our family back to the office, we would like to better understand your thoughts and concerns surrounding the COVID-19 pandemic and returning to the workplace. Please take the time to fill out this survey by October 8th to better understand both the comfort level and the sentiment towards returning.

Return_to_work_survey

As part of the state of Florida Stay Safe Plan, all businesses require a COVID-19 Preparedness Plan which includes this survey. If you would like to provide additional dialogue on the topic, please leave additional comments at the end, and we will reach out to address any concerns.

Best Regards,

John Smith | Corporate HR Manager

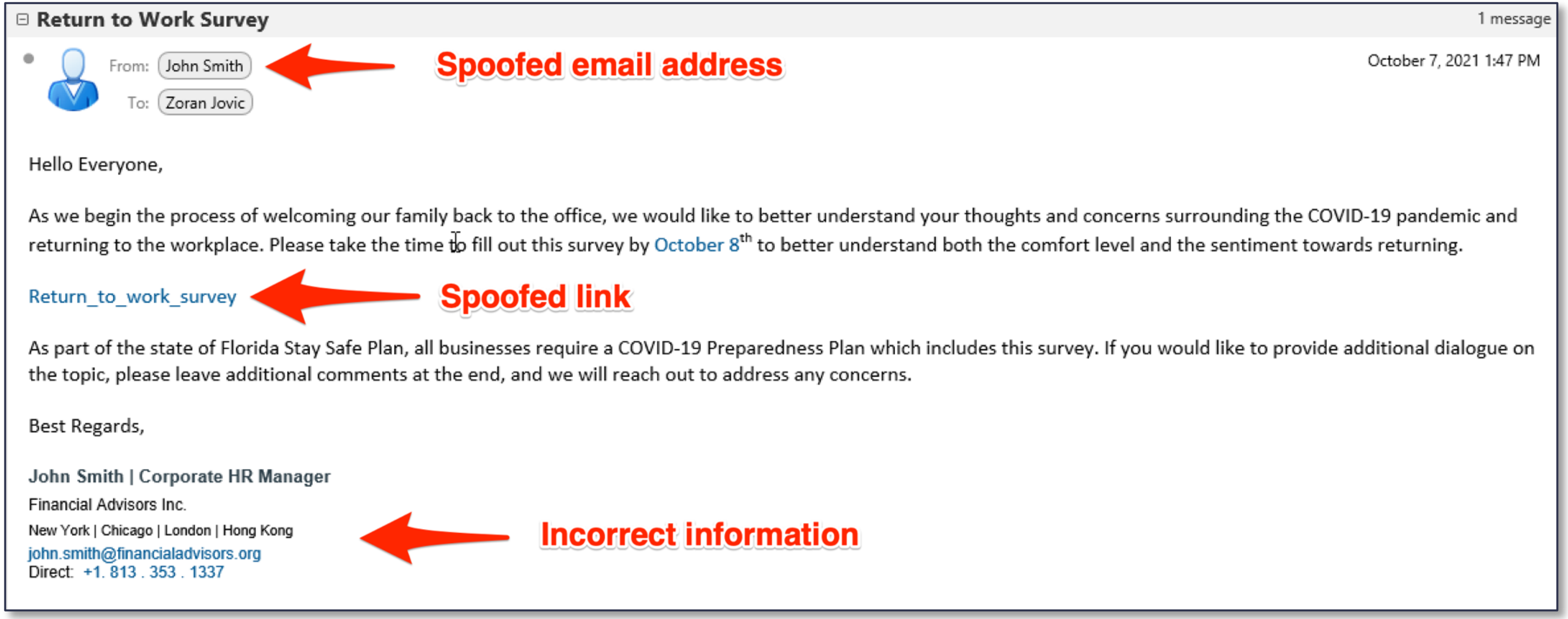
Financial Advisors Inc.

New York | Chicago | London | Hong Kong

john.smith@financialadvisors.org

Direct: +1. 813 . 353 . 1337

Spoofed Links/Email



⊟ **Return to Work Survey** 1 message

From: John Smith

To: Zoran Jovic

October 7, 2021 1:47 PM

Spoofed email address

Hello Everyone,

As we begin the process of welcoming our family back to the office, we would like to better understand your thoughts and concerns surrounding the COVID-19 pandemic and returning to the workplace. Please take the time to fill out this survey by October 8th to better understand both the comfort level and the sentiment towards returning.

Return_to_work_survey

Spoofed link

As part of the state of Florida Stay Safe Plan, all businesses require a COVID-19 Preparedness Plan which includes this survey. If you would like to provide additional dialogue on the topic, please leave additional comments at the end, and we will reach out to address any concerns.

Best Regards,

John Smith | Corporate HR Manager
Financial Advisors Inc.
New York | Chicago | London | Hong Kong
john.smith@financialadvisors.org
Direct: +1. 813 . 353 . 1337

Incorrect information

Minimize the Risk of Phishing

1. Staff Security Awareness Program
   - Don’t trust links or attachments
   - Ensure you are visiting the website you think you are visiting
   - Don’t browse the web/check email as an administrator
   - If something looks odd… check it before you click it!

2. Technical Controls
   - Filter emails and domains
   - Implement email sandboxing
   - Utilize Multi Factor Authentication (MFA/2FA)

Credential Compromise

Password Attacks

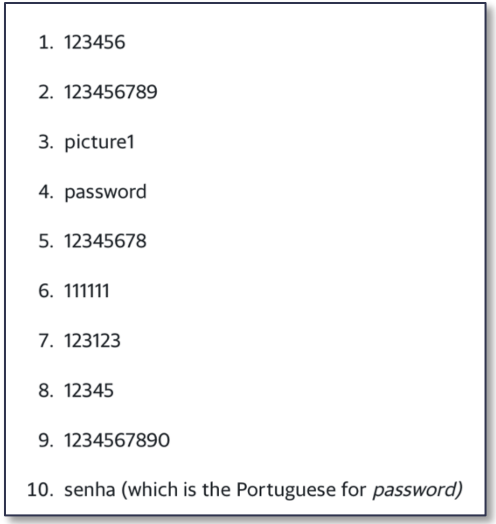
WEALTH ADVISORY | OUTSOURCING
AUDIT, TAX, AND CONSULTING

Investment advisory services are offered through CliftonLarsonAllen
Wealth Advisors, LLC, an SEC-registered investment advisor

Password Guessing

- Users choose predictable passwords
  - “Seasonal Defective Password Disorder”: *Summer2021!*
  - Common substitutions: *P@ssw0rd*
  - Organization name: *CLAUniversity1*

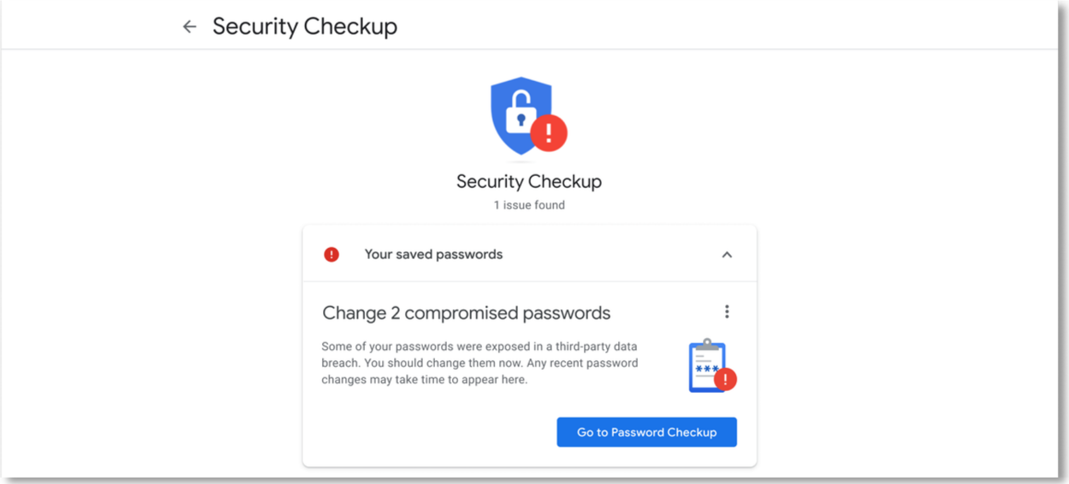
- List of top passwords does not change much YoY



1. 123456
2. 123456789
3. picture1
4. password
5. 12345678
6. 111111
7. 123123
8. 12345
9. 1234567890
10. senha (which is the Portuguese for *password)*

Password Reuse

- Same password being used across accounts
  - Often across personal and business email accounts
  - 44 million Microsoft users reused passwords in the first three months of 2019 *



← Security Checkup

Security Checkup

1 issue found

Your saved passwords

Change 2 compromised passwords

Some of your passwords were exposed in a third-party data breach. You should change them now. Any recent password changes may take time to appear here.

Source: Microsoft 2019

Polling Question 2:

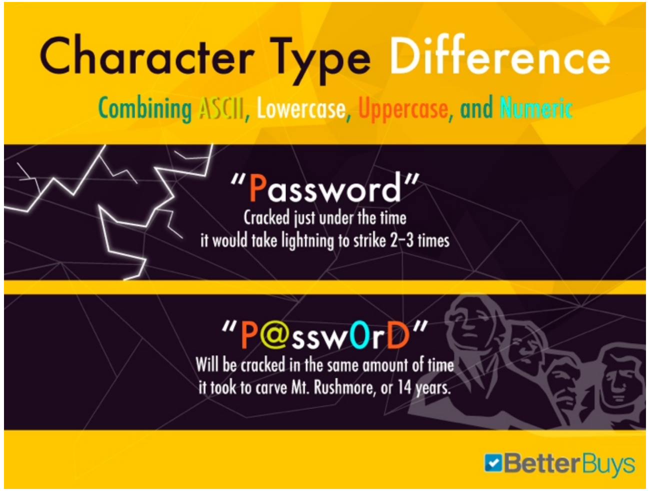
Do currently have any accounts (social media, work, banking…) that share a password?

a. Yes, sharing some passwords
b. No, not sharing any passwords
c. Only sharing passwords amongst <u>work accounts</u>
d. Only sharing passwords amongst <u>personal accounts</u>

Password Cracking

- Password Hash
  - Passwords are stored in an encrypted format (Hash) - unique value for each password
    - *P@ssw0rD > DF3C25A62D926F27B08C6D6B8A9F02BA*

- Password Cracking
  - Attackers must “decrypt” to get the password
    - *Guess > Compute Hash > Compare*



Character Type Difference

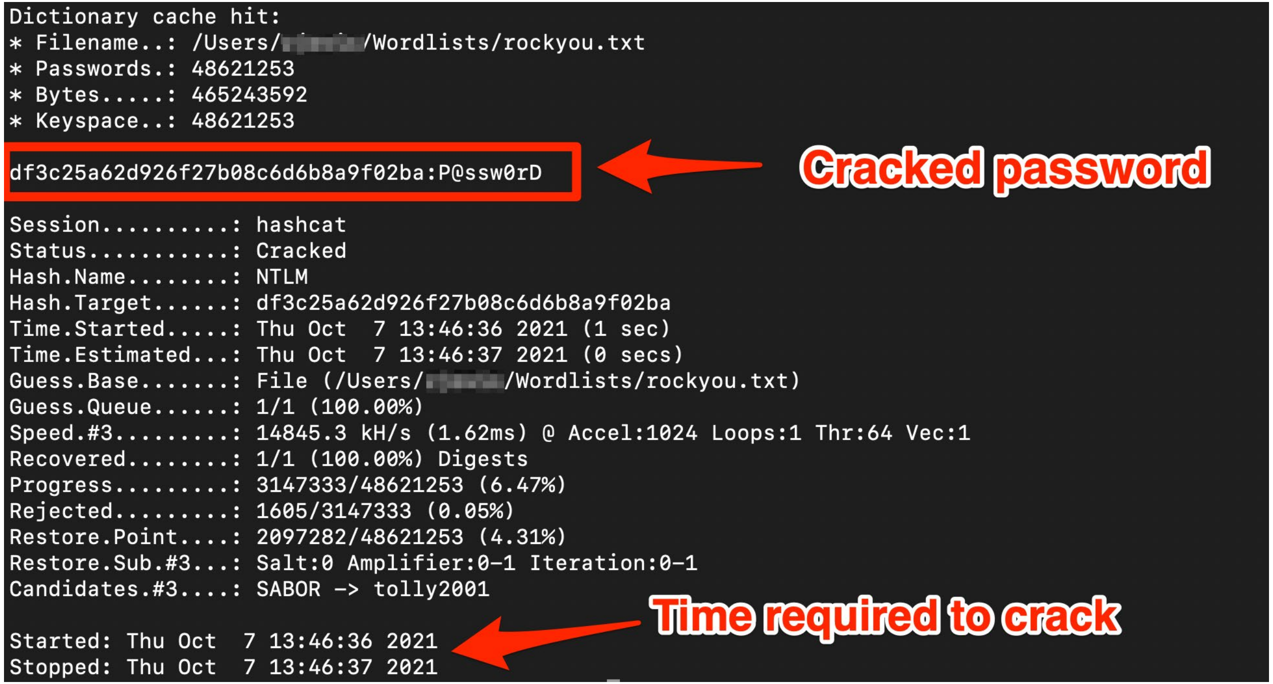
Combining ASCII, Lowercase, Uppercase, and Numeric

“Password”
Cracked just under the time
it would take lightning to strike 2-3 times

“P@ssw0rD”
Will be cracked in the same amount of time
it took to carve Mt. Rushmore, or 14 years.

BetterBuys

14 Years to Crack “*P@ssw0rD*”???



```
Dictionary cache hit:
* Filename..: /Users/[redacted]/Wordlists/rockyou.txt
* Passwords.: 48621253
* Bytes.....: 465243592
* Keyspace..: 48621253

df3c25a62d926f27b08c6d6b8a9f02ba:P@ssw0rD

Session..........: hashcat
Status...........: Cracked
Hash.Name........: NTLM
Hash.Target......: df3c25a62d926f27b08c6d6b8a9f02ba
Time.Started.....: Thu Oct  7 13:46:36 2021 (1 sec)
Time.Estimated...: Thu Oct  7 13:46:37 2021 (0 secs)
Guess.Base.......: File (/Users/[redacted]/Wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#3.........: 14845.3 kH/s (1.62ms) @ Accel:1024 Loops:1 Thr:64 Vec:1
Recovered........: 1/1 (100.00%) Digests
Progress.........: 3147333/48621253 (6.47%)
Rejected.........: 1605/3147333 (0.05%)
Restore.Point....: 2097282/48621253 (4.31%)
Restore.Sub.#3...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidates.#3....: SABOR -> tolly2001

Started: Thu Oct  7 13:46:36 2021
Stopped: Thu Oct  7 13:46:37 2021
```

Cracked password

Time required to crack

Steps to Mitigate Password Attacks

1. Use a long and strong password
   - Minimum 14 characters with complexity ***
   - Avoid using “bad words”… CompanyName, SeasonYear, PetName…
   - Use a “pass phrase” – had to guess, easy to remember

2. Use a unique password for each app/site
   - Do not use work credentials as login for personal business

3. Use password security tools
   - Password manager
   - Multi-factor authentication (MFA/2FA)

Controls to Mitigate the Risk

WEALTH ADVISORY | OUTSOURCING
AUDIT, TAX, AND CONSULTING

Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor

What can Leadership Do about Phishing?

1. Implement Security/Technical Controls
   - ○ Reduce the likelihood of a user making a mistake

2. Implement a Continuous User Awareness Program
   - ○ User susceptibility to phishing decreases over time

3. Inspect and Verify
   - ○ Is your phishing training producing the desired results?
   - ○ Simulate an attack and test your Incident Response
   - ○ Perform a Risk Assessment

What can Leadership Do about Passwords?

1. Implement and Enforce proper policies
   - Minimum 14 characters with complexity
   - Explicitly prohibit password reuse
   - Implement password training during onboarding and on ongoing basis
     - All stakeholders must be included - students

2. Implement technical controls
   - Tools can prevent users from choosing a compromised or easily guessable password
   - Deploy password managers and MFA/2FA

3. Inspect and Verify
   - Perform regular password audits

Questions

WEALTH ADVISORY | OUTSOURCING
AUDIT, TAX, AND CONSULTING

Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor

Thank you!

Kadian Douglas
CISA, CPA
Principal – Cybersecurity Services
Direct: 813-384-2735
Kadian.Douglas@claconnect.com

David Anderson
OSCP
Principal – Cybersecurity Services
Direct: 612-376-4699
David.Anderson@claconnect.com

Zoran Jovic
GPEN
Consultant – Cybersecurity Services
Direct: 813-384-2728
Zoran.Jovic@claconnect.com

CLAconnect.com

WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING

Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor

Create Opportunities

> CLA exists to
> create opportunities —
> for our clients, our people,
> and our communities.

WEALTH ADVISORY | OUTSOURCING
AUDIT, TAX, AND CONSULTING

Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor