



We'll get you there.

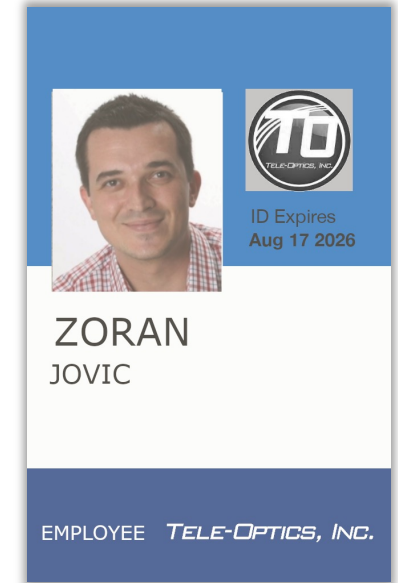
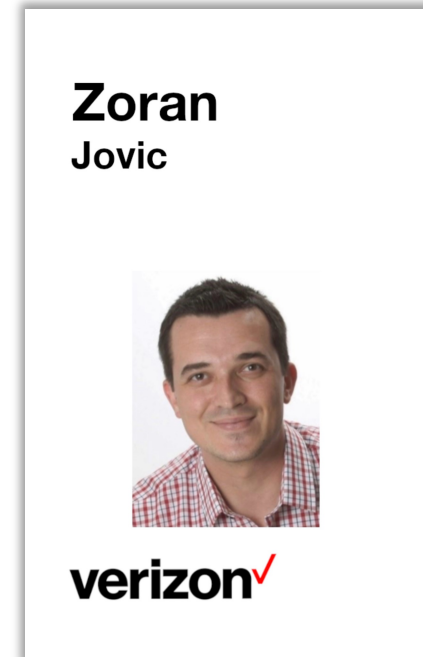
CPAs | CONSULTANTS | WEALTH ADVISORS

Reducing the Risk of a Cyberattack

2024 WTBA Annual Convention

Zoran Jovic

- Cybersecurity consultant @ CLA
- Manage and oversee team of cybersecurity consultants
- Enjoy social engineering!
- US Army veteran



Cybersecurity Services at CLA

Cybersecurity Security offered as specialized service offering for over 25 years

- Penetration Testing and Vulnerability Assessment
- IT/Cyber security risk assessments
- IT audit and compliance (HIPAA, GLBA/FFIEC, NIST, CMMC, CIS, etc.)
- PCI-DSS Readiness and Compliance Assessments (PCI-DSS)
- Incident response and forensics
- Independent security consulting
- Internal audit support



Objectives

- Identify potential risks and consequences of cybersecurity vulnerabilities and attacks
- Review strategies for recognizing and avoiding social engineering (email phishing) attempts
- Identify password vulnerabilities and learn what make a password 'strong'
- Learn how existing tools can reduce the risk of an attack





Cyber Attacks & “Cybercrime”

Common Cyber Attacks

Phishing

- *Step one in many attacks*
- **Method:** Voice, Email, Text, Search Engine, “Spear”
- **Effect:** Attacker receives login credentials, implants malicious software to device, potentially leading to other attacks.

Ransomware Attacks

- **Attack Method:** Phishing, Infected USB Drives, visiting malicious sites
- **Effect:** Unusable resources

DDoS (Distributed Denial of Service)

Method: Overloading of dummy/fake requests to a targeted server (or multiple) forcing it unusable.

Effect: Disturbance and unusable systems until remediated.

Data Breach

- **Attack Method:** Phishing, lost or stolen devices, insider threats, malware
- **Effect:** Loss of data, regulatory sanctions

Potential effects of attacks: Reputational, financial, legal/regulatory sanctions



Cybercrime and Black-Market Economies

- Black market economy to support cyber fraud
 - Business models and specialization
 - Underground Marketplace (The Dark Web)
- Most common cyber fraud scenarios
 - Theft of information
 - Log-in Credentials
 - ePHI, PII, PFI, account profiles, etc.
 - Credit card information
 - Ransomware
- To the Hackers, we all look the same...

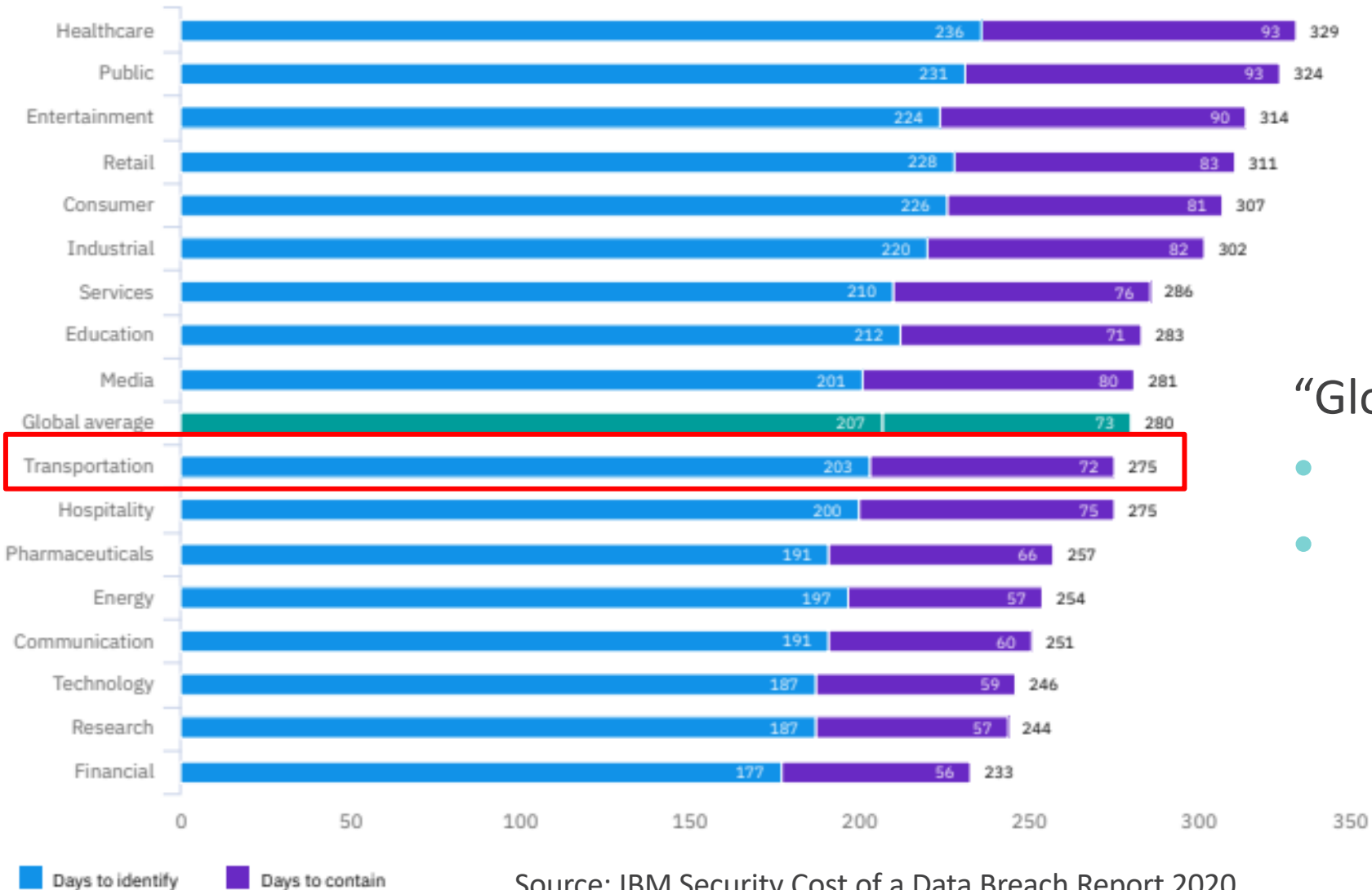


They will hit you with any or all of the following:

1. Email Spear Phishing Attacks
2. Password Guessing and Business Email Account Takeovers
3. Payment and Funds Disbursement Transfer Fraud
4. Ransomware
5. Extortion to avoid breach disclosure



Average Days to Identify and Contain a Data Breach



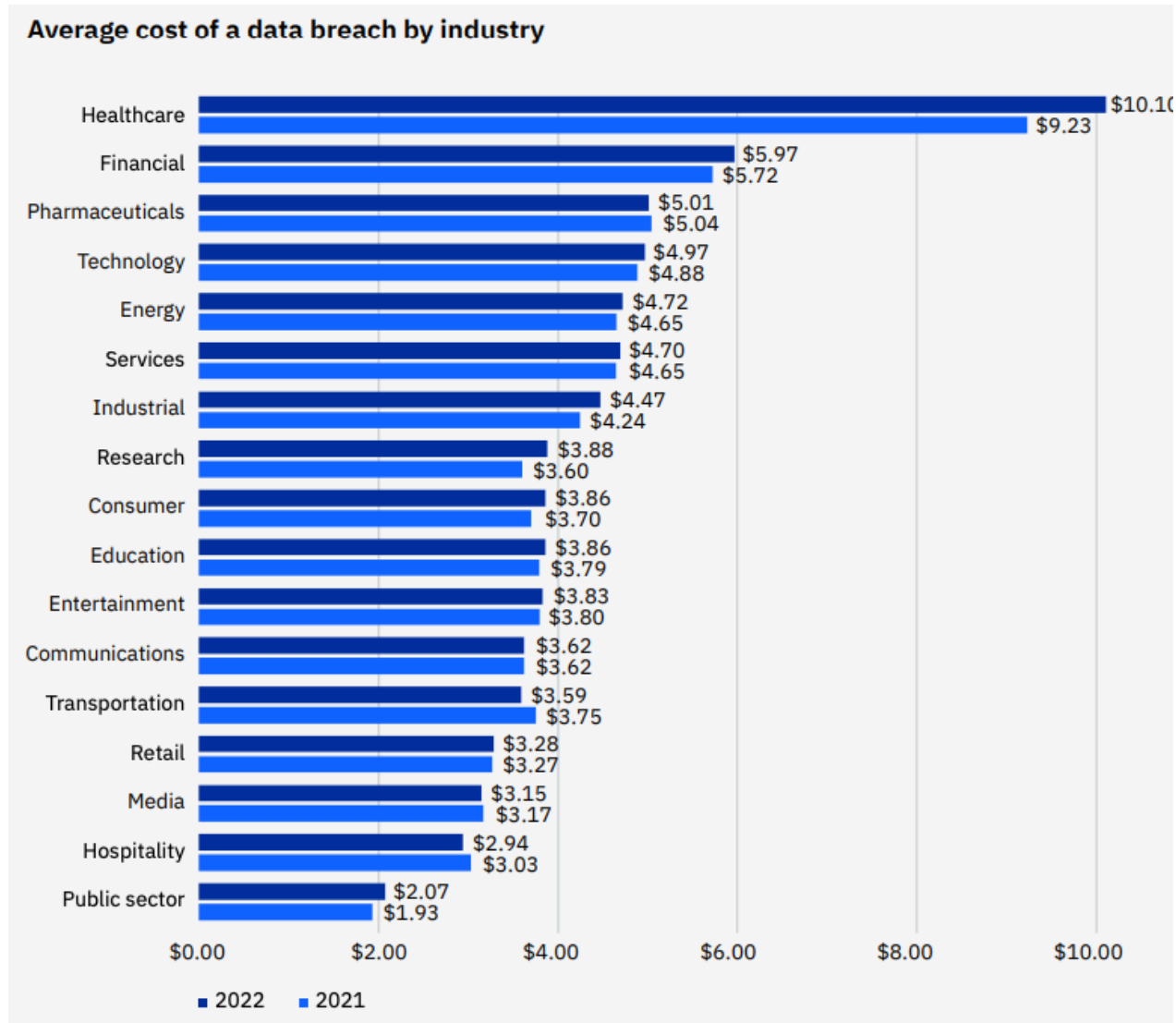
“Global” average is 280 days

- 203 days to identify a breach
- 72 days to contain the attack

Source: IBM Security Cost of a Data Breach Report 2020



Average Cost of a Data Breach



Factors

- Lost business cost
- Detection & escalation
- Post breach response
- Notification

Source: IBM Security Cost of a Data Breach Report 2022



Behind the statistics

- Hackers can do a lot in AND to your network in 200+ days
 - Learn everything about you and your organization
 - Find your crown jewels and take them
 - Disable backups and security systems
 - Create numerous back doors
 - Attack everyone you are connected to



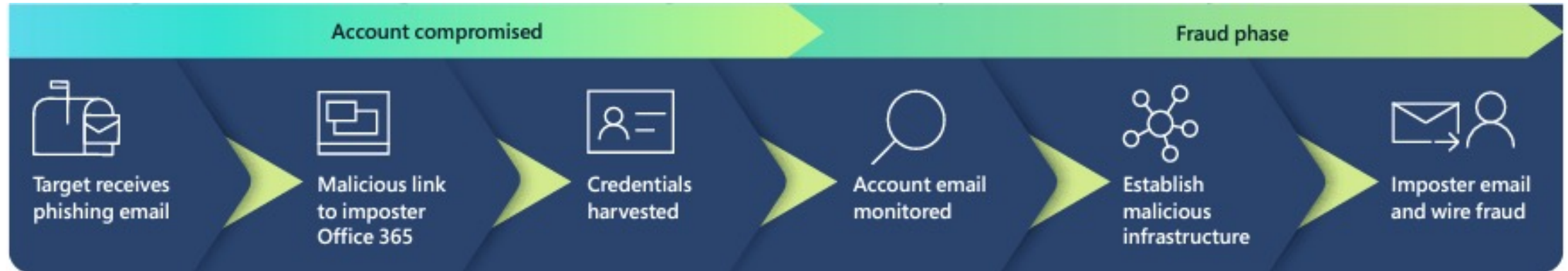
Email Phishing

What is Email Phishing?

- Attackers impersonate ‘trusted entities’ via email to deceive recipients into divulging sensitive information
- Phishing emails appear legitimate, mimicking branding, logos, and language of trusted organizations
- Phishing emails often contain links to fake websites or attachments containing malware
- Rely on psychological tactics like urgency or fear to prompt immediate action from victims



Email Compromise Timeline



- Credentials = Access
- Gathering user credentials is generally the goal
- The credentials are then sold or traded on the dark web

Microsoft 2022 Digital Defense Report



Credentialed phishing schemes on the rise – indiscriminately target all inboxes



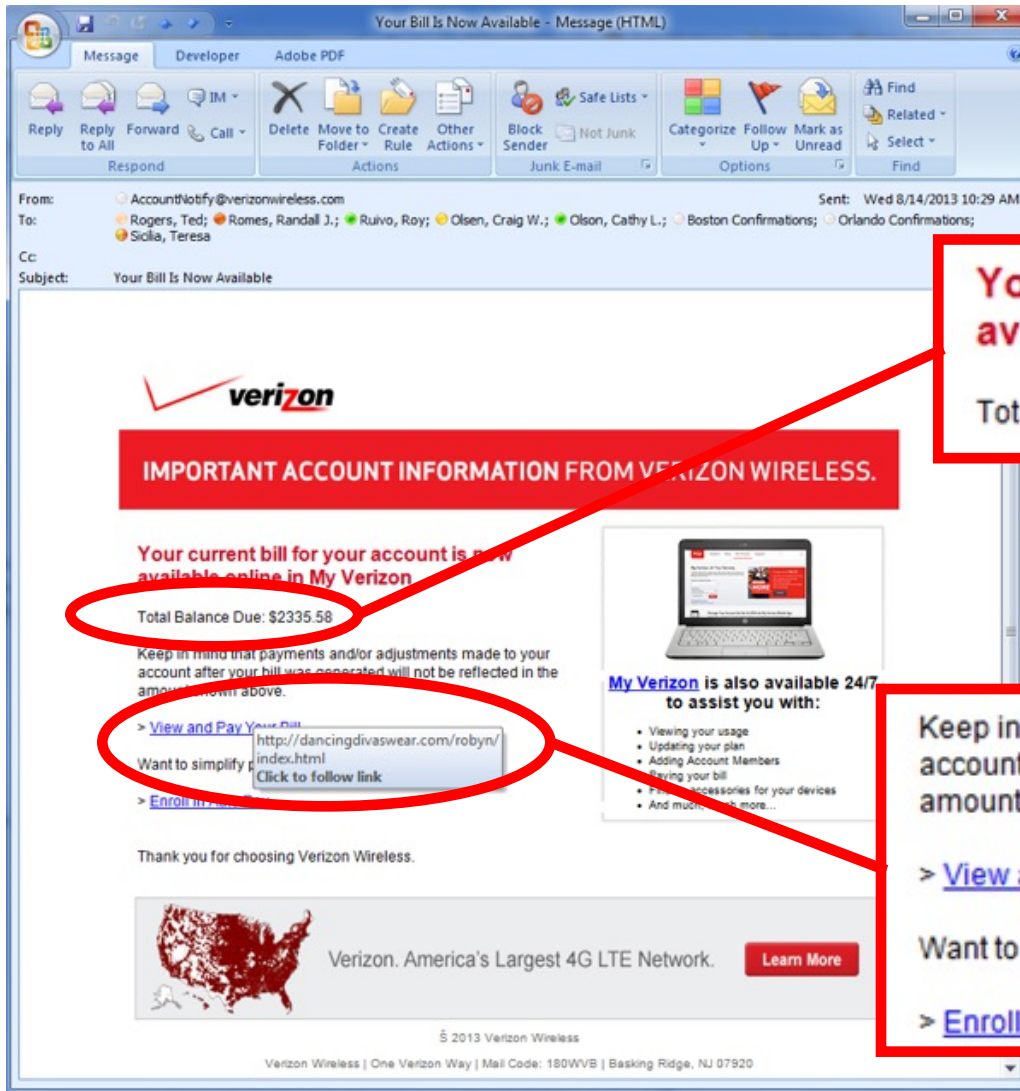
The volume of phishing attacks is orders of magnitude **greater than all other threats**



710 million phishing emails blocked per week



Emotional Response Required!



Your current bill for your account is now available online in My Verizon

Total Balance Due: \$2335.58

IMPORTANT ACCOUNT INFORMATION FROM VERIZON WIRELESS.

Your current bill for your account is now available online in My Verizon

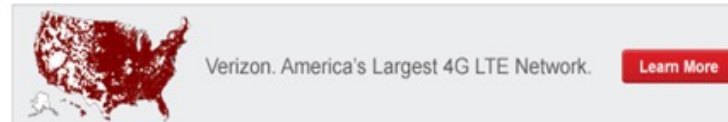
Total Balance Due: \$2335.58

Keep in mind that payments and/or adjustments made to your account after your bill was generated will not be reflected in the amount shown above.

> [View and Pay Your Bill](http://dancingdivaswear.com/robyn/index.html)
http://dancingdivaswear.com/robyn/index.html
Click to follow link

> [Enroll in Auto Pay](#)

Thank you for choosing Verizon Wireless.



© 2013 Verizon Wireless

Verizon Wireless | One Verizon Way | Mail Code: 180WVB | Basking Ridge, NJ 07920

My Verizon is also available 24/7 to assist you with:

- Viewing your usage
- Updating your plan
- Adding Account Members
- Paying your bill
- Finding accessories for your devices
- And much, much more...

Keep in mind that payments and/or adjustments made to your account after your bill was generated will not be reflected in the amount shown above.

> [View and Pay Your Bill](http://dancingdivaswear.com/robyn/index.html)
http://dancingdivaswear.com/robyn/index.html
Click to follow link

> [Enroll in Auto Pay](#)



”Accidental” Email Example

Employee Compensation Adjustment List 1 message

From: [Redacted] Dawn November 5, 2020 9:53 AM

To: [Redacted] ← Sent to EVERYONE in the company

BJ,

Below is the modified list of employees scheduled to receive out-of-cycle compensation adjustments as we previously discussed. Royce and I discussed and made a few updates.

[Employee-Comp-Adjustments-2020-11-05.docx](#)

Please let me know if you have any questions or want to discuss further. These adjustments will start on November 9th.

Regards,

Dawn



Business Email Compromise

- Fraudsters impersonate employees, service providers, or vendors via email in an attempt to...
 - Steal or transfer \$\$\$
 - Authorize a distribution
 - Impersonate an Executive asking staff to “buy gift cards”
 - Update direct deposit account

Fw: Commission Payment



o Dwayne Pearse <dwayne@vendor.com>

To: o Brian Johnson



Download All

Preview All

This message is high priority.

EXTERNAL

We have an update in receiving payments, Via ACH. Kindly advice how we effect this change immediately.

Dwayne Pearse
dwayne@vendor.com
549-555-2232

From: Dwayne Pearse <dwayne@vendor.com>
Sent: Thursday, December 12, 2019 2:15 PM
To: William Bergson <william@vendor.com>; Barb Rogers <barbara@vendor.com>
Subject: FW: Commission Payment

From: Brian Johnson <bjohnson@company.com>
Date: Thursday, December 12, 2019 at 2:14 PM
To: Dwayne <dwayne@vendor.com>, William Bergson <william@vendor.com>
Subject: Commission Payment

Good afternoon,

Attached is the backup for commissions paid from the company.

Brian Johnson
Accounts Payable Supervisor
bjohnson@company.com

Spoofing with Homoglyph

- Replacing characters to make email addresses or web sites look legitimate
- A homoglyph address looks identical to a real address the victim recognizes is registered on a mail provider with a username that is identical

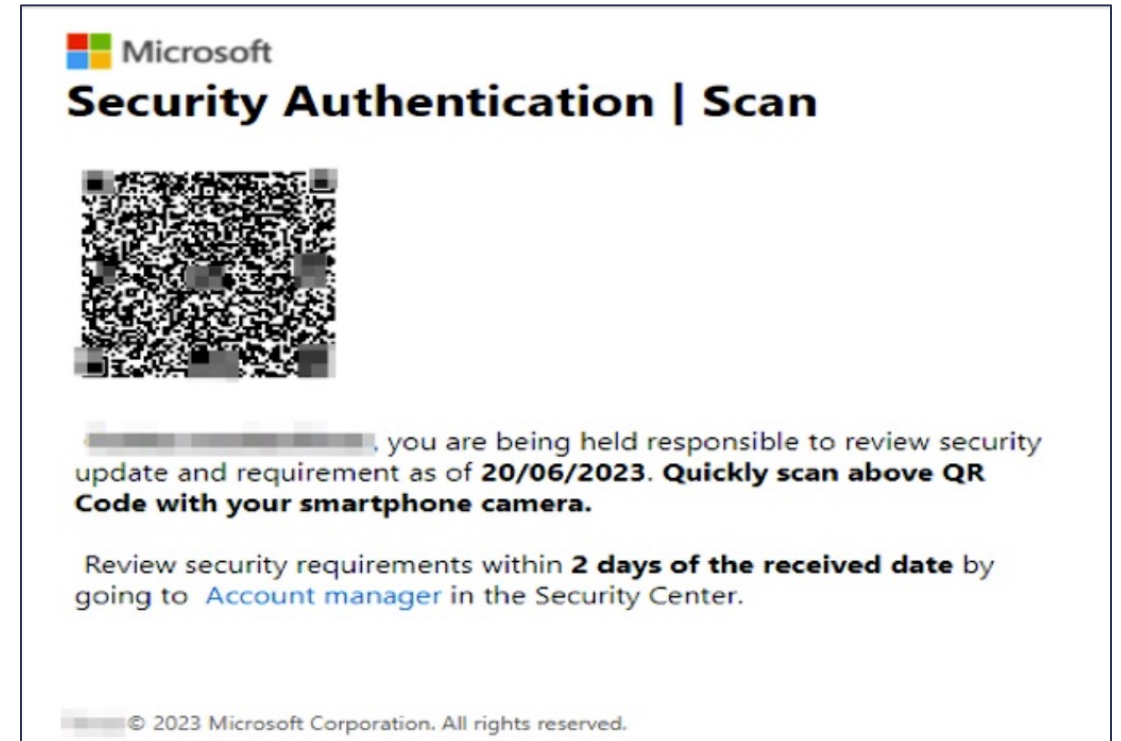
Technique	% of domains showing homoglyph technique
sub l for I	25%
sub i for l	12%
sub q for g	7%
sub rn for m	6%
sub .cam for .com	6%
sub 0 for o	5%
sub ll for l	3%
sub ii for i	2%
sub vv for w	2%
sub l for ll	2%
sub e for a	2%
sub nn for m	1%
sub ll for l, sub l for i	1%
sub o for u	1%

Analysis of over 1,700 homoglyph domains between January–July 2022. While 170 homoglyph techniques were used, 75% of domains used just 14 techniques.



QR Phishing

- Emails contain a PDF or image of a QR code
- QR emails are much harder to detect and block



Identify Suspicious Emails

- Generic greetings
- Spelling or grammatical errors
- Suspicious email addresses or domains
- Requests for personal information
- Be cautious of email attachments and links
- Avoid clicking links or downloading files!



Avoiding Social Engineering

- Be skeptical and question requests
- Independently verify the legitimacy of any requests
- Be wary of urgency and high-pressure tactics
- Be cautious about sharing sensitive information
- Hover over links (without clicking) to inspect the actual destination address



Utilize Technology!

- Implement Multi-Factor Authentication (MFA)
- Keep software and computer updated
- Employ security tools like spam filters, firewalls, and antivirus software
- Provide/attend regular, periodic, cybersecurity awareness training(s)





Password Compromise

What is Password Compromise?

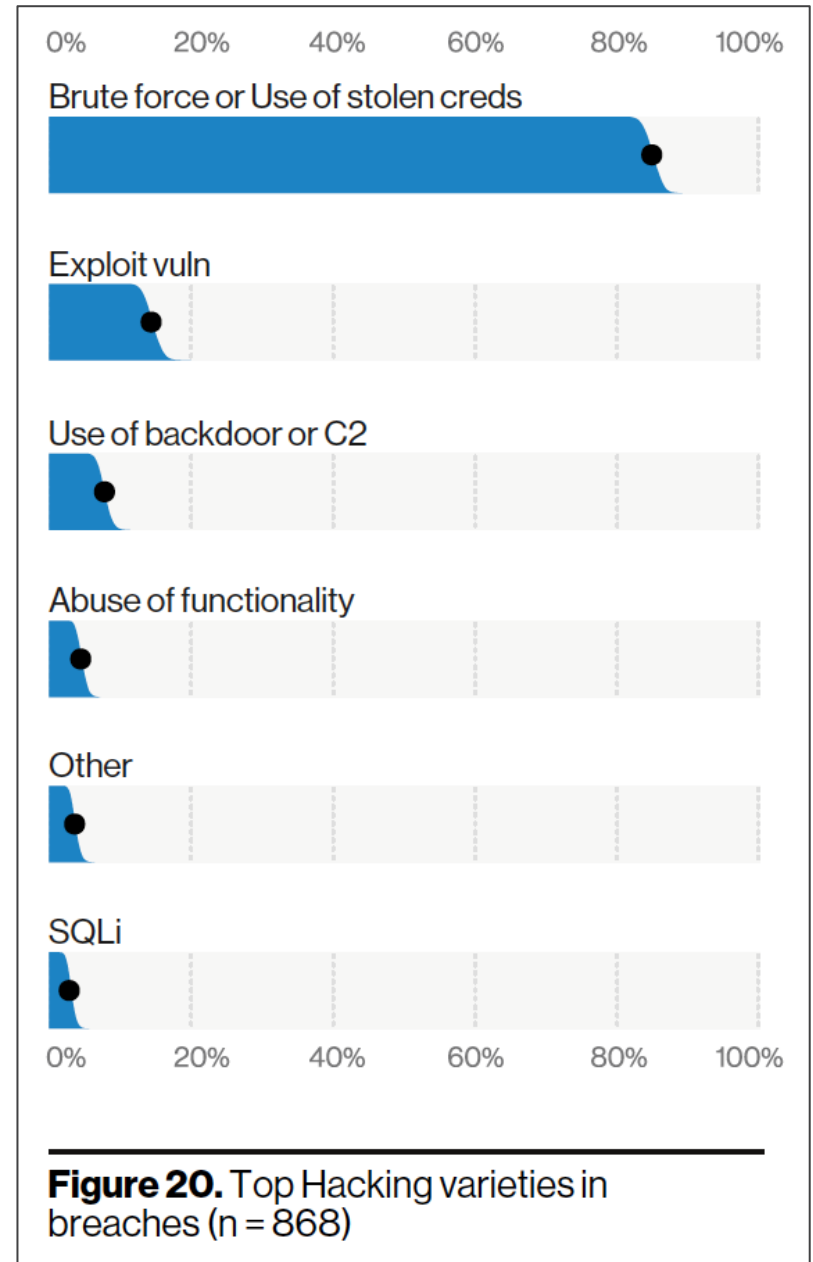
- Unauthorized access to a user's password to gain access to sensitive accounts or systems
- Often occurs through various means such as phishing
- Most commonly password compromise is enabled by:
 - Reusing passwords across multiple accounts
 - Choosing 'bad' passwords
 - Choosing short passwords



Passwords

- 80% of data breaches involved compromising user credentials
- Simple tools to steal and guess credentials

Source: 2022 Verizon DBIR



Give Me Your Creds

- Microsoft 365 credentials remain one of the most highly sought after account types for attackers
- Once compromised attackers can log in to corporate-tied computer systems

1hr 12 m

The median time it takes for an attacker to access your private data if you fall victim to a phishing email

1hr 42 m

The median time for an attacker to begin moving laterally within your corporate network once a device is compromised



Password Challenge

Password1

Summer2023

IHatePasswords!

ClasTheBestInTheUSA!

CLA!\$@m@z!ng

H!p21Y@wn!ng95\$v(



Passwords

➤ Old Rules (NIST)

- Length (8+ characters)
- Complexity (A a 4 @)
- Forced expiration (every__days)

➤ New Guidance (NIST)

- Passphrases
- Password tools
 - MFA
 - Password managers

Password Audit	Total
Number of passwords audited	855
Passwords cracked	794
Passwords that were all letters	63
Passwords that were all numbers	5
Passwords that were an English word	20
Passwords that were a word with numbers appended to it	200
Passwords that were the same as the username	6
Passwords that do not meet Windows complexity	584




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” the hash
 - *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.

 Better Buys 

14 Years to Crack “P@ssw0rD”???

```
Host memory required for this attack: 345 MB
```

```
Dictionary cache hit:
```

```
* Filename..: /Users/zjovic/Wordlists/rockyou.txt
```

```
* Passwords.: 48621253
```

```
* Bytes.....: 465243592
```

```
* Keyspace..: 48621253
```

```
df3c25a62d926f27b08c6d6b8a9f02ba:P@ssw0rD
```

Cracked password

```
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/zjovic/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
```

Time required to crack



Password Strategies:

- **Pass Phrases – Loooooong natural language**

Password23 <----- **Unforgivable!**

Summer23 <----- **Terrible**

*N*78fm/12f* <----- **Painful**

Wallet Painting lamp <-- **GOOD**

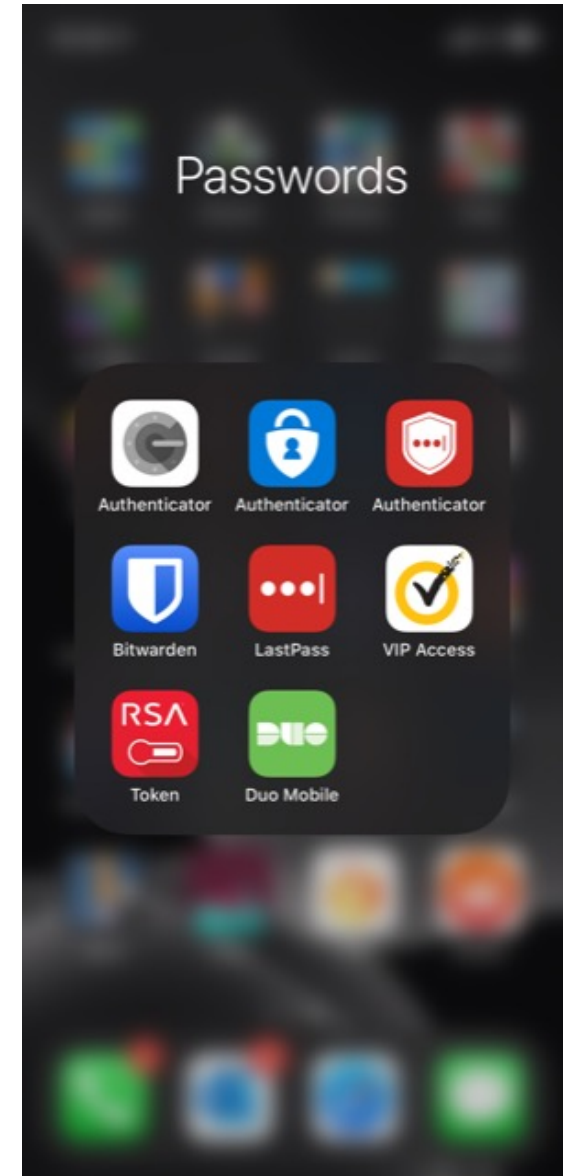
In 2023 we will win the Superbowl! ← **BEST**

- Password tools: **Password Managers** are needed



Multi-Factor Authentication (MFA)

- All remote systems/applications should require MFA
 - Email, VPN, Remote Desktop, Banking, etc.
- Not all MFA is created equal
 - Number matching, push notifications, phone calls, SMS text, soft token (6 digit code), etc.



Protect your credentials!

Use looong passwords/passphrases

Do not reuse passwords

Use multi factor authentication and password managers

Geo-Restrict and System-restrict access to email if possible

Most importantly: Don't use obvious passwords!!!





Questions?

Thank You!

Zoran Jovic, GPEN
Manager, Cybersecurity
813-947-9656
Zoran.Jovic@CLAconnect.com



CLAconnect.com



CPAs | CONSULTANTS | WEALTH ADVISORS

©2023 CliftonLarsonAllen LLP. CLA (CliftonLarsonAllen LLP) is an independent network member of CLA Global. See [CLAglobal.com/disclaimer](https://www.claglobal.com/disclaimer).
Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor.