“THAR SHE BLOWS!”

SPEARPHISHING, WHALING, AND EVERYTHING IN BETWEEN

XACT DATA DISCOVERY
Because you need to know

WELCOME

- Thank you for joining
- 300+ registrants from wide range of organizations and roles
- Please feel free to submit questions using question box
- Slides, recording and survey coming tomorrow via email

XACT DATA DISCOVERY
Because you need to know

TODAY'S SPEAKER

- **Paul Price**, VP of Forensics
  Xact Data Discovery

  - Manages extensive XDD forensic team
  - Expert in digital forensics and cyber security
  - Conducts digital forensic investigations for civil litigation, criminal matters, internal investigations, and cyber security efforts
  - Certified computer forensic examiner
  - Former law enforcement officer
  - Supervised 1000+ forensic exams
  - Experienced in digital forensics, financial crimes investigation, crime scene, and counterterrorism as a former member of the FBI's Joint Terrorism Task Force

XACT DATA DISCOVERY
Because you need to know

PROGRAM OVERVIEW

- Phishing (Spear Phishing)
- Whaling
- Business Email Compromise (BEC)
- Vishing
- Pretexting

XACT DATA DISCOVERY
Because you need to know

NIGERIAN 419 SCAMS

I am a wealthy Nigerian Prince, all I want to do is give people money but no one believes me! What should I do?

SPEARPHISHING, WHALING, AND EVERYTHING IN BETWEEN

PHISHING

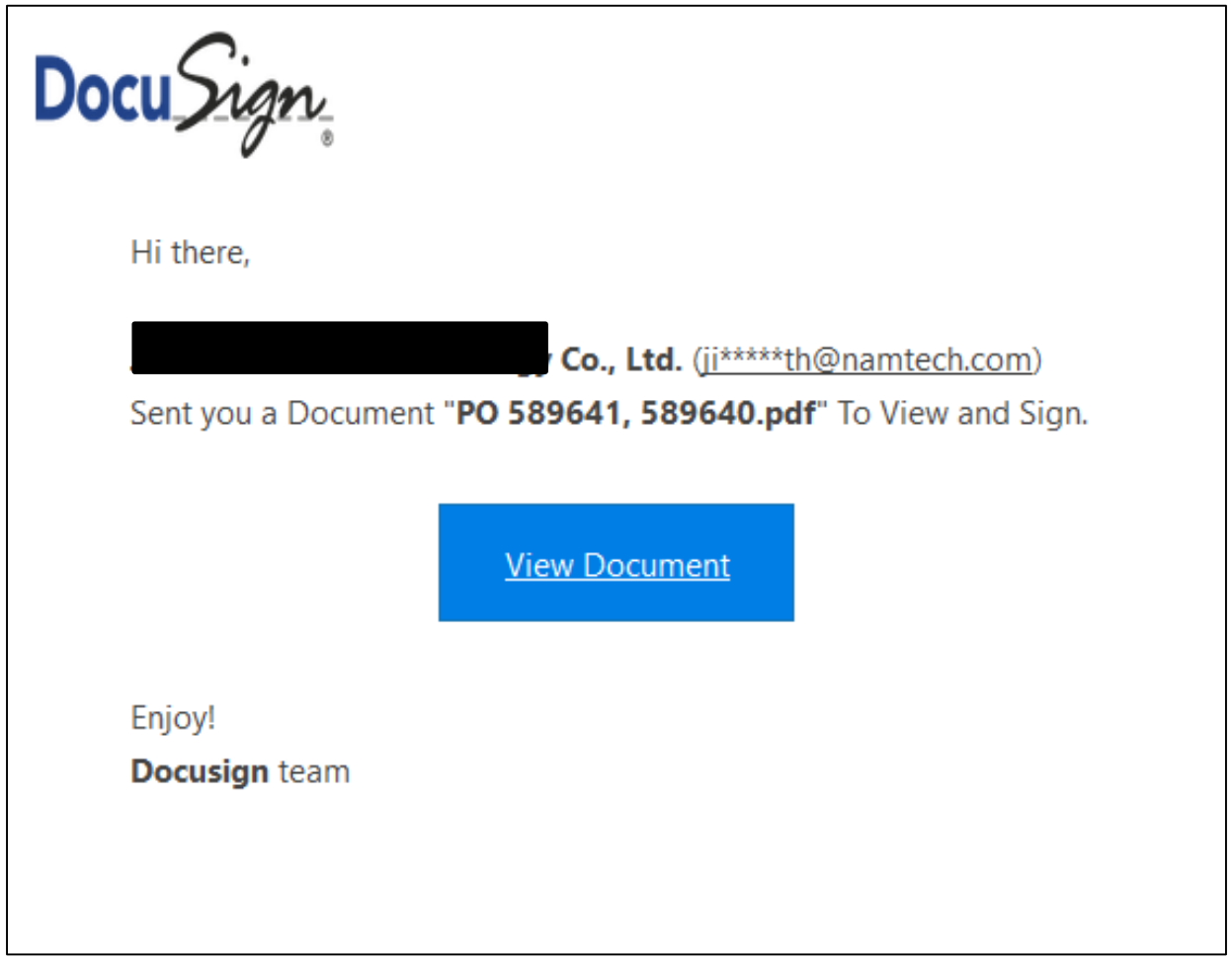
XACT DATA DISCOVERY
Because you need to know

PHISHING

- **Phishing** is highly successful tactic used by cybercriminals to obtain sensitive information from unsuspecting victims
- It uses "bait" such as legitimate appearing emails, text messages, phone calls or websites to request information (i.e. username/password, bank account number, personal information, etc.)
- The messages are seemingly so urgent, so potentially disastrous that the recipient feels compelled to act quickly, putting normal security hygiene practices by the wayside
- **Spear Phishing** is a subset of phishing, using similar methods but targets key individuals who are expected to have very special access or information that the cybercriminal wants
- **91% of successful breaches started with a spear phishing attack!!!**

XACT DATA DISCOVERY
Because you need to know

DOCUSIGN SAMPLE



DocuSign

Hi there,

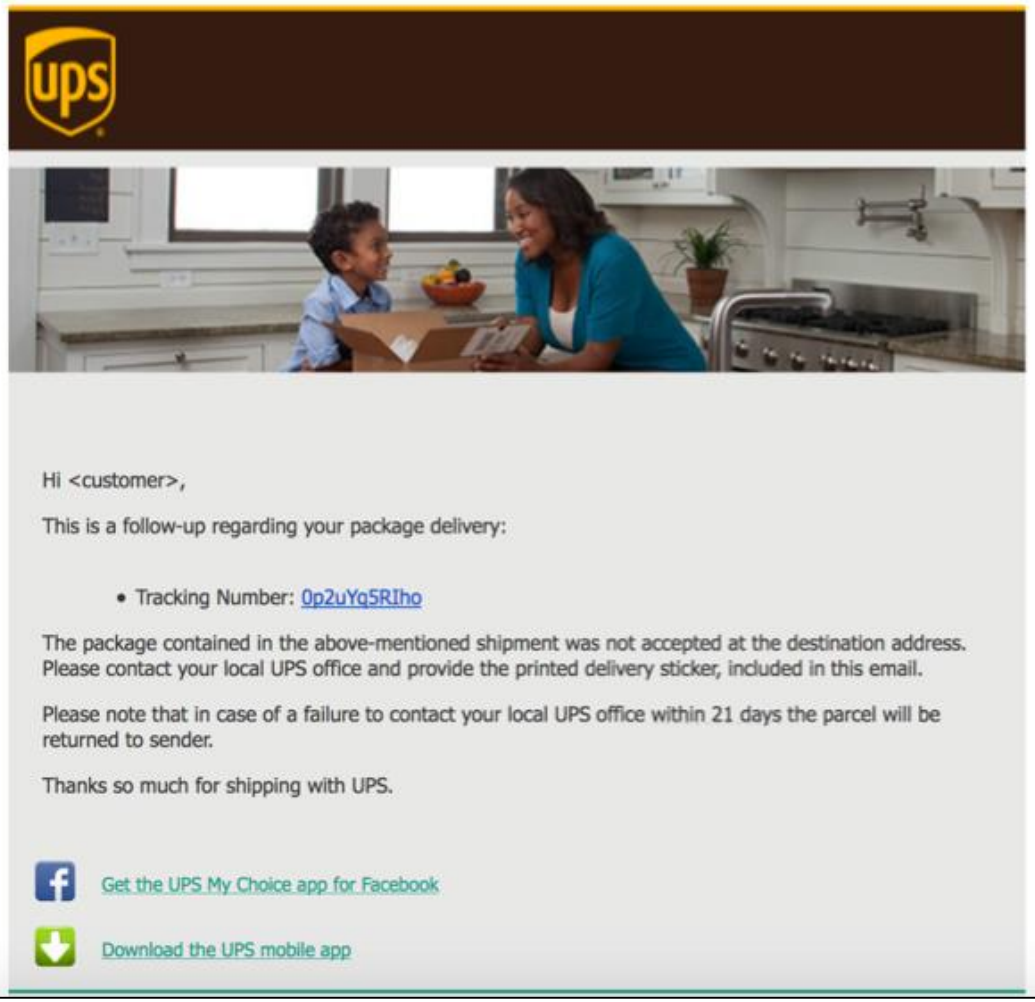
[redacted] Co., Ltd. (ji*****th@namtech.com)
Sent you a Document "**PO 589641, 589640.pdf**" To View and Sign.

View Document

Enjoy!
Docusign team

XACT DATA DISCOVERY
Because you need to know

UPS SAMPLE



Hi <customer>,

This is a follow-up regarding your package delivery:

- Tracking Number: 0p2uYq5RIho

The package contained in the above-mentioned shipment was not accepted at the destination address. Please contact your local UPS office and provide the printed delivery sticker, included in this email.

Please note that in case of a failure to contact your local UPS office within 21 days the parcel will be returned to sender.

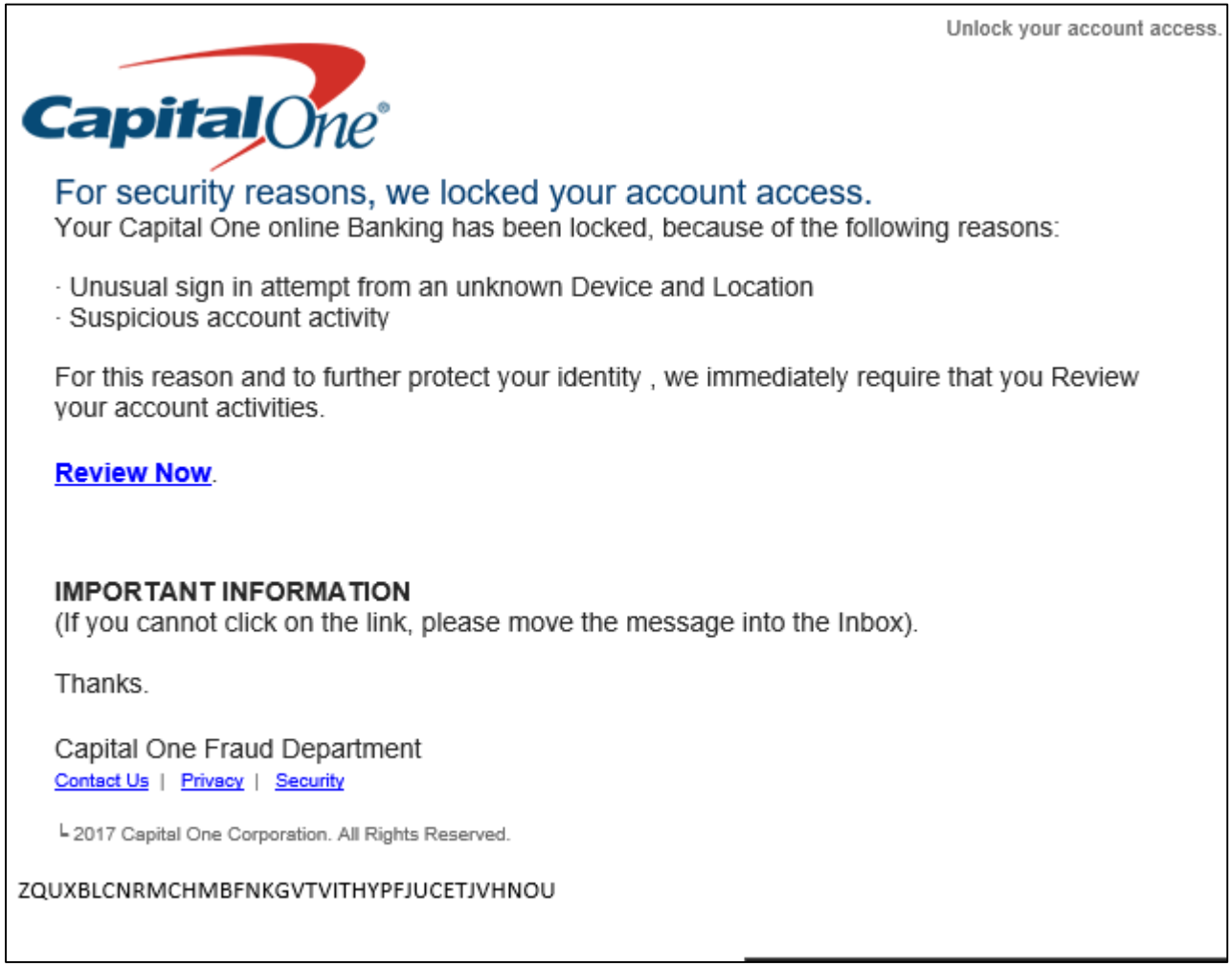
Thanks so much for shipping with UPS.

Get the UPS My Choice app for Facebook

Download the UPS mobile app

XACT DATA DISCOVERY
Because you need to know

WHATS IN YOUR WALLET?



Unlock your account access.

Capital One

For security reasons, we locked your account access.

Your Capital One online Banking has been locked, because of the following reasons:

· Unusual sign in attempt from an unknown Device and Location
· Suspicious account activity

For this reason and to further protect your identity , we immediately require that you Review your account activities.

Review Now.

IMPORTANT INFORMATION
(If you cannot click on the link, please move the message into the Inbox).

Thanks.

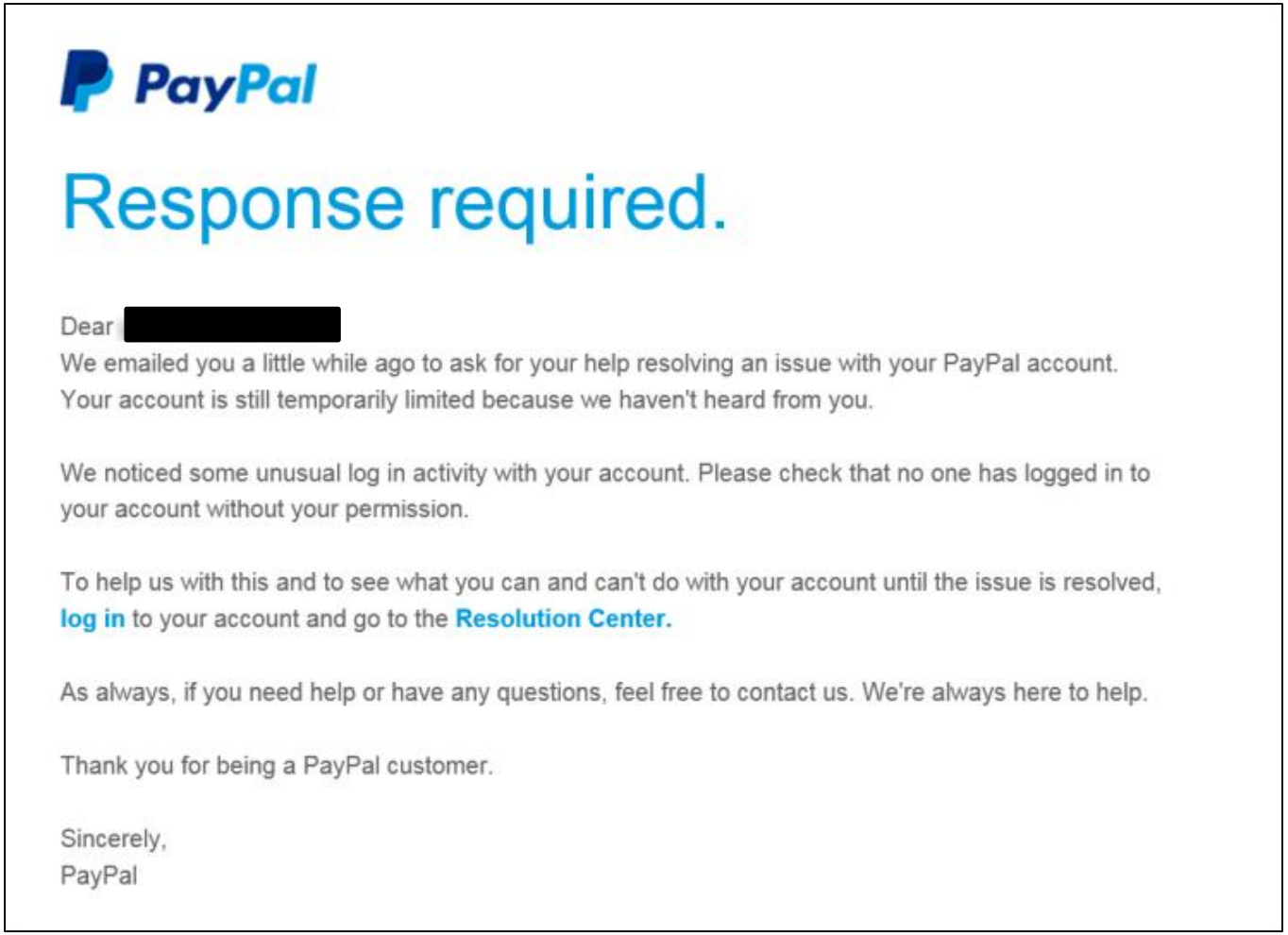
Capital One Fraud Department
Contact Us | Privacy | Security

└ 2017 Capital One Corporation. All Rights Reserved.

ZQUXBLCNRMCHMBFNKGVTVITHYPFJUCETJVHNOU

XACT DATA DISCOVERY
Because you need to know

PAYPAL SAMPLE



PayPal

Response required.

Dear [redacted]
We emailed you a little while ago to ask for your help resolving an issue with your PayPal account. Your account is still temporarily limited because we haven't heard from you.

We noticed some unusual log in activity with your account. Please check that no one has logged in to your account without your permission.

To help us with this and to see what you can and can't do with your account until the issue is resolved, **log in** to your account and go to the **Resolution Center.**

As always, if you need help or have any questions, feel free to contact us. We're always here to help.

Thank you for being a PayPal customer.

Sincerely,
PayPal

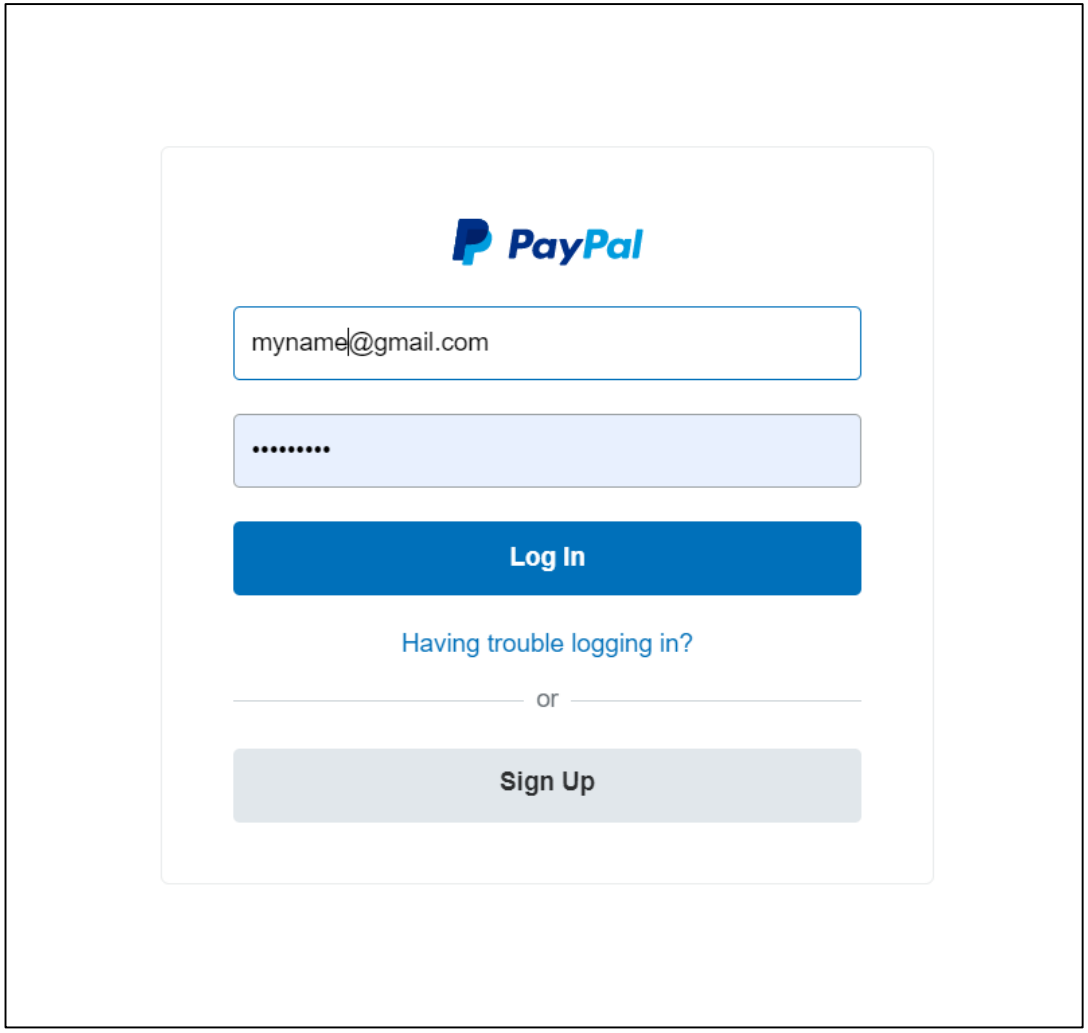
XACT DATA DISCOVERY
Because you need to know

LINKS

- A link (or hyperlink) is a set of directions telling your computer or device where to go once it is clicked on
- They are generally represented by a button on words that are colored differently that the rest of text on the page
- log in = https://u7576412.ct.sendgrid.net/ls/click?upn=sicptvkoqo8zlh8c8phs5tpcjf0cbmlqf543jnlsbsgje-2bce9l2mwjtkdfot1y3wh7g0_yv0ls-2b-2bjzix4u9tkxbtopkdm4h0ldgz6shduql6c4un1lwgxkn2f9bpaxaecrtrbqtjohix7yd1ewaxgba-2bpvmjx5hvjrcm5arx24hchgqgzz-2fawx3rqoy0qx-2bjefblpnw5o5oqkj1g-2fmawv1gohx0khtkfgg9nqpp-2bcjph5mymjvzeed0x2cgj7e5ztb2po-2fpflyd2lerovngpdduourjapqcbnlt-2bpas1ft18xw1q-3d
Click or tap to follow link. = go to my fake site

XACT DATA DISCOVERY
Because you need to know

FAKE SITE



SPEARPHISHING, WHALING, AND EVERYTHING IN BETWEEN

WHALING

XACT DATA DISCOVERY
Because you need to know

WHALING

- Whaling is just another form of phishing for high-value targets such as C-suite executives. The attack is either run against the executive or by impersonating an executive (normally CEO) to get employees to transfer information or company funds.
- Successful whaling attacks demand more time, research, and sophistication than standard phishing
- Attacks against executives generally use common concerns or fears that require a quick response such as legal action or being the subject of reputational harm

XACT DATA DISCOVERY
Because you need to know

WHALING

The New York Times

"Thousands of high-ranking executives across the country have been receiving e-mail messages this week that appear to be official subpoenas from the United States District Court in San Diego. Each message includes the executive's name, company and phone number, and commands the recipient to appear before a grand jury in a civil case".

XACT DATA DISCOVERY
Because you need to know

WHALING

From: United States District Court [subpoena@uscourts.com]
To: [redacted]
Cc:
Subject: Subpoena in case #28-755-YCH

AO: (Rev. 11/94) Subpoena in Civil Case

Issued by the
United States District Court

Issued to: [redacted]

SUBPOENA IN A CIVIL CASE

Case number: 28-755-YCM
United States District Court

YOU ARE HEREBY COMMANDED to appear and testify before the Grand Jury of the United States District Court at the place, date, and time specified below.

Place:	United States Courthouse 880 Front Street	Date and Time:	May 7, 2008 9:00 a.m. PST

SPEARPHISHING, WHALING, AND EVERYTHING IN BETWEEN

WHALING/BUSINESS EMAIL COMPROMISE

XACT DATA DISCOVERY
Because you need to know

WHALING

- Business Email Compromise (BEC) is also known as CEO Fraud
- Impersonation of executive(s)
- Common targets include CFO, Controller/Comptroller, HR, Accounting/Finance

REAL WORLD CASE SCENARIO

XACT DATA DISCOVERY
Because you need to know

WHALING EXAMPLES

- The payroll department at Snapchat received a whaling email that purported to come from the CEO asking for employee payroll information. In response to the email, the payroll staff disclosed all of the company's payroll data to the attacker.
- Toy giant Mattel lost over $3 million after a senior finance executive fell victim to a whaling email attack. The email purported to come from the new CEO and requested a wire transfer.
- An executive at Seagate responded to a whaling email that requested the W-2 forms for all current and former employees. The incident resulted in a breach of income tax data for nearly 10,000 Seagate employees.

XACT DATA DISCOVERY
Because you need to know

STATISTICS

- In 2017, there was 200% increase noted for Business Email Compromise types of whaling attacks
- In 2019, Phishing and credential theft remain as the prominent attack types
- 98% of all phishing attacks use email
- Financial gain is the most common motive

SPEARPHISHING, WHALING, AND EVERYTHING IN BETWEEN

VISHING

XACT DATA DISCOVERY
Because you need to know

VISHING

- **Vishing** is a type of phishing that uses a fake caller ID or spoofed number to impersonate a business or individual to gain access to sensitive information

XACT DATA DISCOVERY
Because you need to know

VISHING

SPEARPHISHING, WHALING, AND EVERYTHING IN BETWEEN

PRETEXTING

XACT DATA DISCOVERY
Because you need to know

IN PERSON PRETEXTING

- **Pretexting** is tactic used to physically impersonate legitimate individuals in order to gain access to secured areas or computers and steal data
- Attackers generally research targets thoroughly and rely on their ability to communicate to gain and exploit trust for malicious purposes
- Higher personal risk, but still very effective

SPEARPHISHING, WHALING, AND EVERYTHING IN BETWEEN

KEY TAKE-AWAYS

XACT DATA DISCOVERY
Because you need to know

KEY TAKE-AWAYS

- Think before you click – "*When it doubt, Throw it out*"
- Always scrutinize a request for username/password
- Use Two-Factor Authentication (2FA) for everything
- Limit the amount of personal information you make public
- Implement multiple layers of approval for major transactions
- Never access random USB device
- Don't assume someone is who they say they are
- Training…Training….Training

XACT DATA DISCOVERY
Because you need to know

ENGAGE WITH XDD

- XDD email coming tomorrow with slides, recording, survey and invite to next webinar
- RSVP for upcoming webinar on Wednesday, April 29th, at 1PM EDT:
  - ***Time to Make the Donuts: Processing Fundamentals***
    - *Matthew Verga, JD, XDD Director of Education*
    - *Brent Westenfelt, XDD Director, eDiscovery Operations Management*
- Visit the "Learn" section of the XDD website for valuable white papers, blog articles and webinars at www.xactdatadiscovery.com
- Engage with XDD
  - XDD Educational Webinar Topic Survey
  - https://www.xactdatadiscovery.com/xdd-educational-webinar-topic-survey/