Leticia Saiid

Phishing Psychology

KEYS CONFERENCE

1

Disclaimer

A FEW THINGS FIRST

This presentation is for information only.
Evaluate risks before acting based on ideas from this presentation.

This presentation contains opinions of the presenters.
Opinions may not reflect the opinions of Tandem.

This presentation is proprietary.
Unauthorized release of this information is prohibited.

KEYS CONFERENCE

2

Leticia Saiid

Security+, Chief of Staff

KEYS CONFERENCE

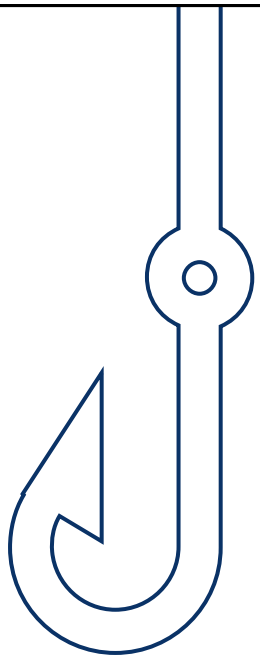
3

4

Agenda

LET'S ANSWER SOME QUESTIONS

- What is phishing?
- What does effective phishing look like?
- Is there a better way to educate on phishing?
- Preparing for Phishing



KEYS CONFERENCE

5

How involved are **YOU** in cybersecurity education?

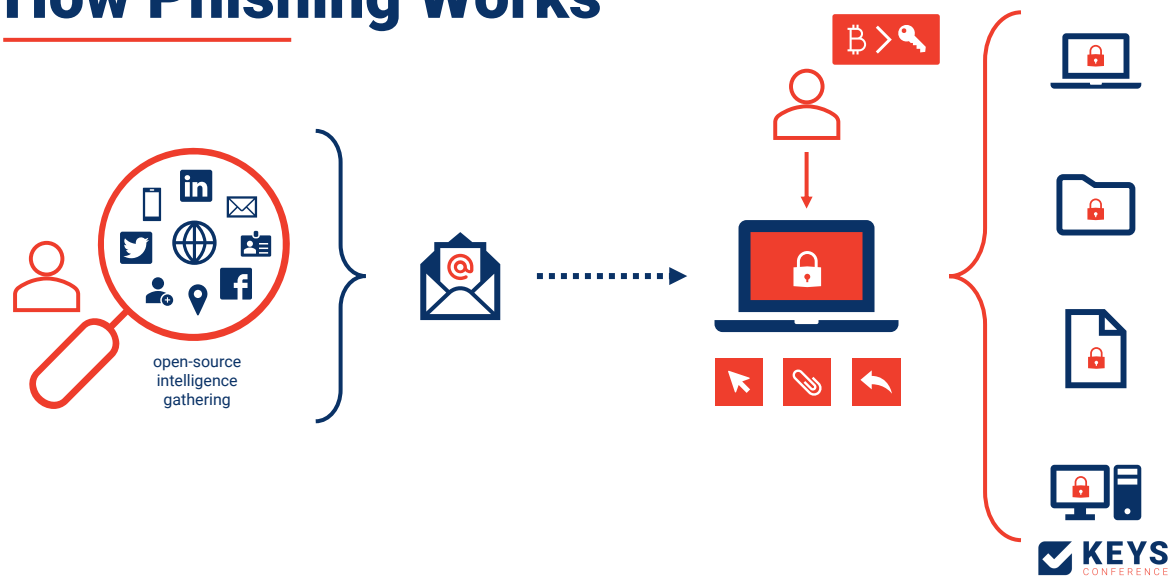
6

KEYS CONFERENCE

What is Phishing?

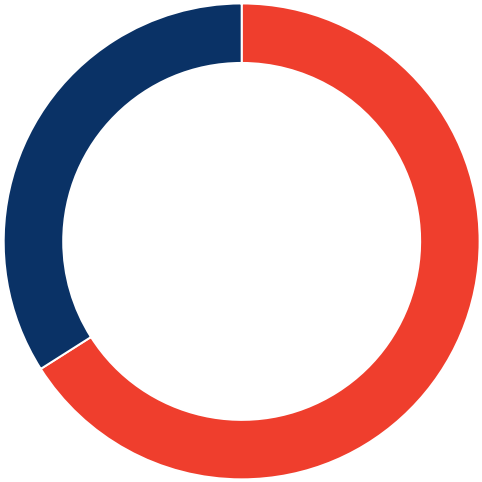
7

How Phishing Works



KEYS CONFERENCE

8



2 out of 3 Ransomware Attacks Begin with Phishing

KEYS CONFERENCE

9

KEYS CONFERENCE

10

COLONIAL PIPELINE HACKERS' STATEMENT

"We are apolitical, we do not participate in geopolitics, **do not need** to tie us with a defined government and look for other our motives. **Our goal is to make money and not creating problems for society.** From today, we introduce moderation and check each company that our partners want to encrypt to avoid social consequences in the future."

https://www.theverge.com/2021/5/10/22428996/colonial-pipeline-ransomware-attack-apology-investigation

KEYS CONFERENCE

11

KEYS CONFERENCE

What does effective phishing look like?

12

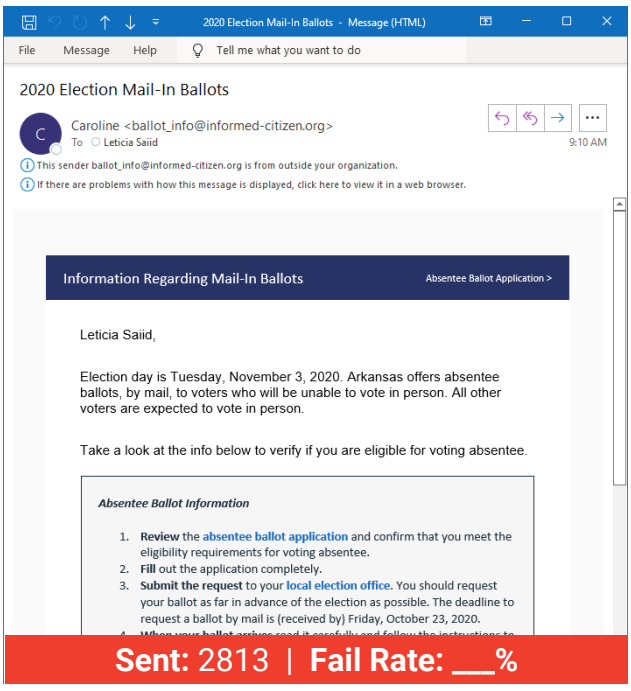
HIGHER

or

LOWER

KEYS CONFERENCE

13



Sent: 2813 | **Fail Rate:** ___%

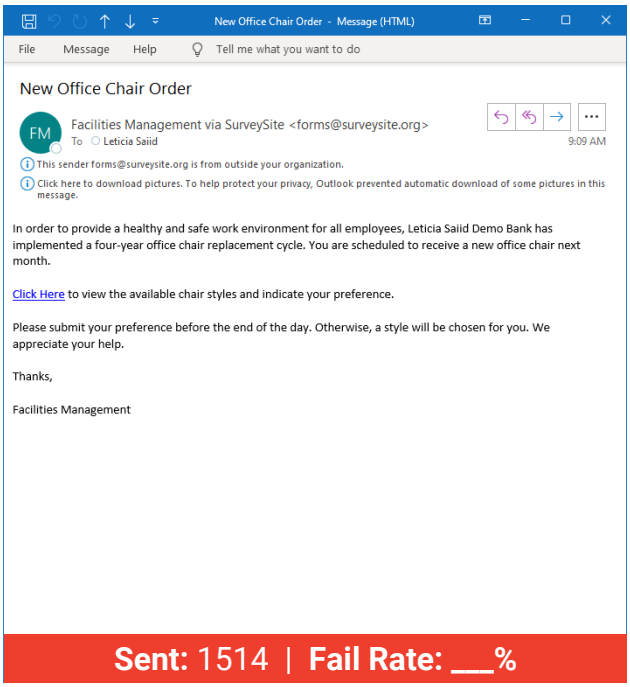
The failure rate for this template in Tandem is

~~10%~~

1.6%

KEYS CONFERENCE

14



The failure rate for this template in Tandem is

~~10%~~

25%

KEYS CONFERENCE

15

Which message has a higher % of failures?

Sent: 374 | **Fail Rate:** 18.98%

Signature needed - Please review COVID related changes to remote work policy

director@bankcompliance.us
To Leticia Saiid
9:01 AM

This sender director@bankcompliance.us is from outside your organization.

Remote Work Policy Update.xlsx
10 KB

Dear Leticia Saiid,

We are updating our remote work policy due to changes in Federal COVID Protocols. Since these changes will affect almost all individuals associated with our company, we are requiring each employee to review the attached document and digitally sign that you have received this notice.

Remote Work Policy Update

Enforcement of the new policy updates will occur 5 business days from the date of this email. Please view and sign the document as soon as possible.

Thank you for your cooperation,
HR Management

1

Sent: 2746 | **Fail Rate:** 0.66%

Keeping You Updated: COVID-19 Boosters

CommunityHealth <info@healthcare-news.org>
To Leticia Saiid
9:00 AM

This sender info@healthcare-news.org is from outside your organization.

CommunityHealth

To our valued patient,

Our top priority is your health and safety, so we want to continue keeping you informed about COVID-19.

As you may have heard, COVID-19 vaccine booster shots are now being recommended for ongoing protection against the virus for high-risk individuals.

Learn more about the recent FDA approval and boosters. Talk with your healthcare provider if you think you might be eligible for a booster shot. Check with your local public health department or see vacinations.gov for more information.

Thank you for trusting us as your partner in health.

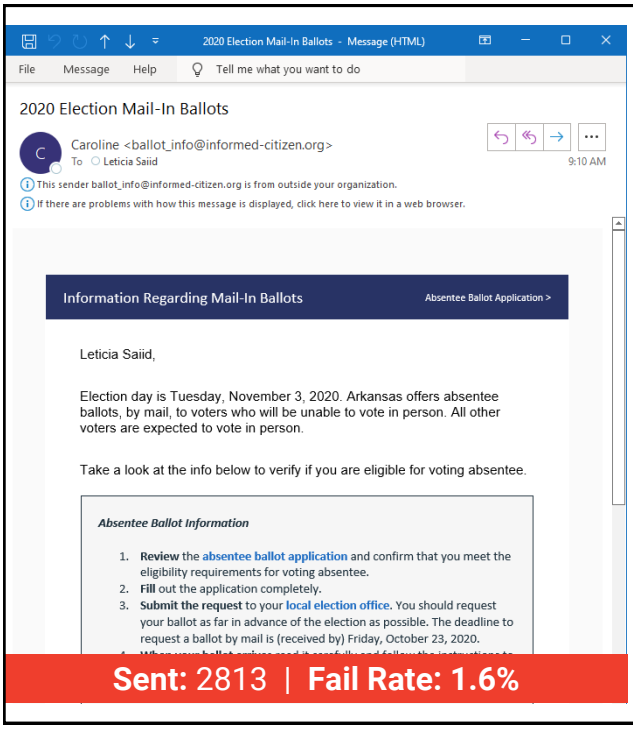
UNSUBSCRIBE OR UPDATE PREFERENCES | PRIVACY POLICY

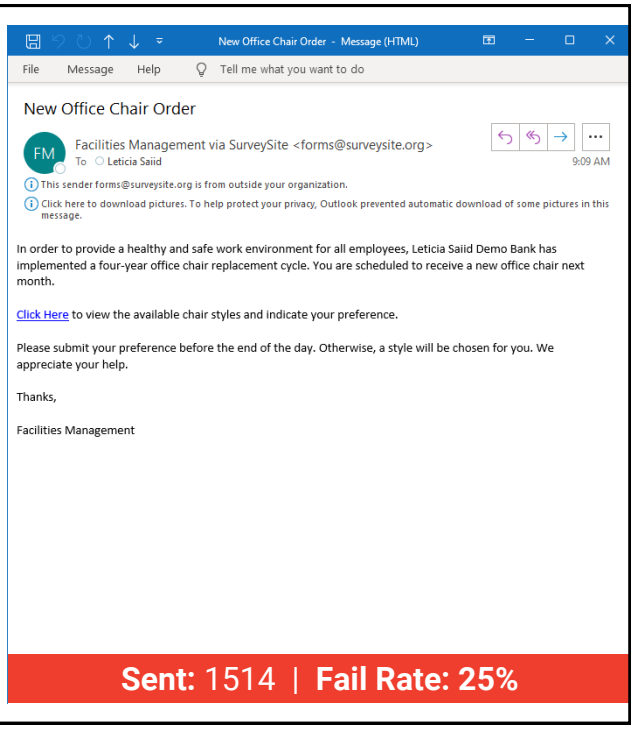
If you'd rather not receive emails like these, you can unsubscribe from our mailing list by clicking "unsubscribe" above.

© CommunityHealth
5000 Southeast Medical Parkway

2

16



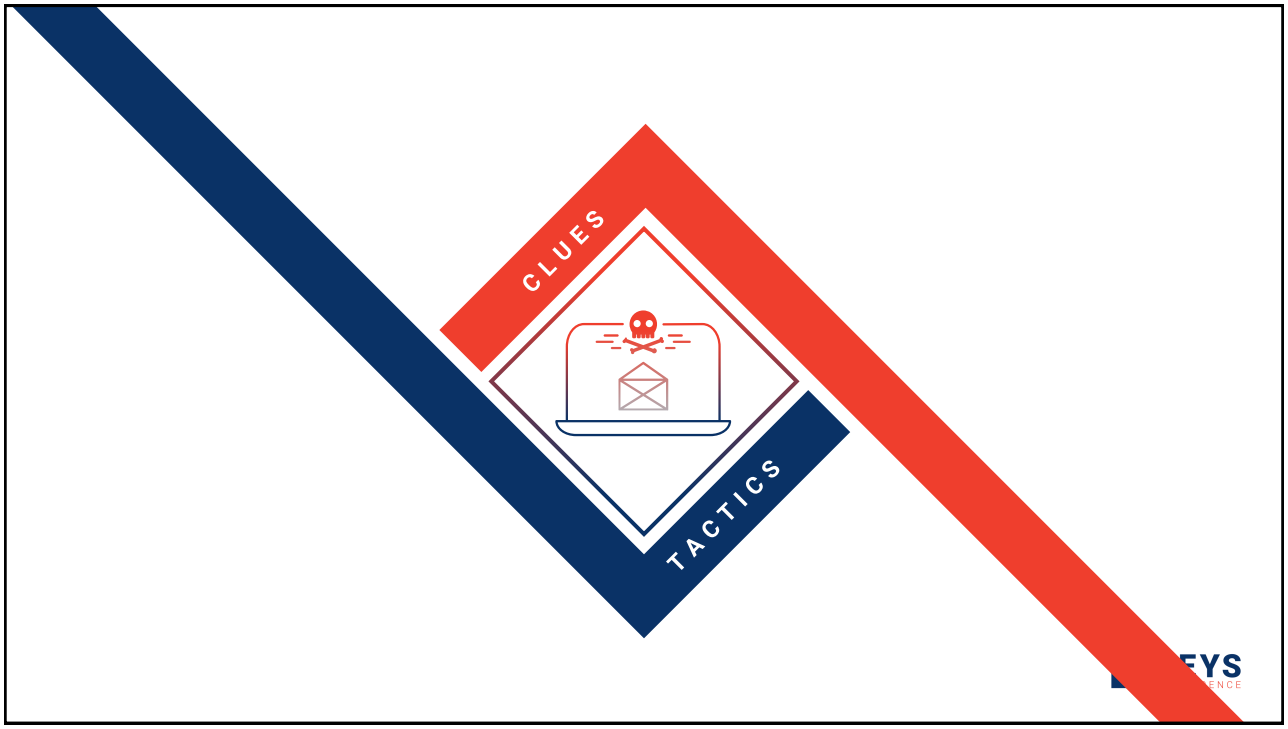


17

KEYS CONFERENCE

Is there a better way to educate on phishing?

18



19

When You Receive an Email…

CHECK FOR CLUES

Things which are clearly wrong with the email.

BEWARE OF TACTICS

Distractions to make you act without thinking.

KEYS CONFERENCE

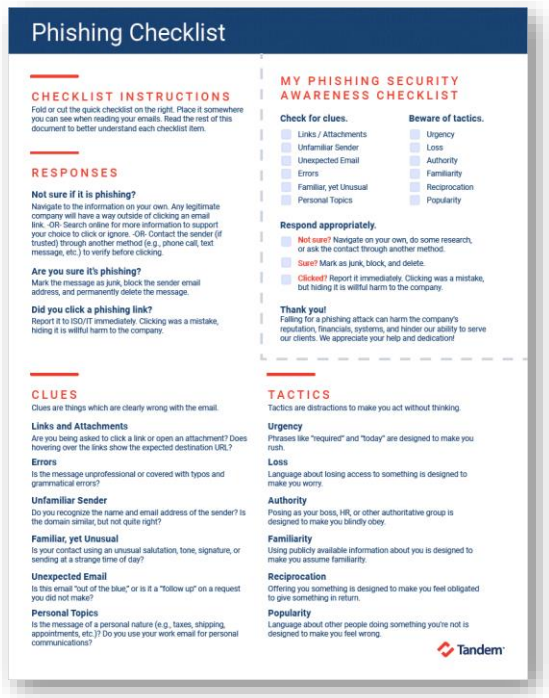
20

How to catch a phisher:

- **C** Clues
- **A** And
- **T** Tactics
- **C** Can
- **H** Help

KEYS CONFERENCE

21



Phishing Checklist

CHECKLIST INSTRUCTIONS

Fold or cut the quick checklist on the right. Place it somewhere you can see when reading your emails. Read the rest of this document to better understand each checklist item.

RESPONSES

Not sure if it is phishing?
Navigate to the information on your own. Any legitimate company will have a way outside of clicking an email link. -OR- Search online for more information to support your choice to click or ignore. -OR- Contact the sender (if trusted) through another method (e.g., phone call, text message, etc.) to verify before clicking.

Are you sure it's phishing?
Mark the message as junk, block the sender email address, and permanently delete the message.

Did you click a phishing link?
Report it to ISO/IT immediately. Clicking was a mistake, hiding it is willful harm to the company.

MY PHISHING SECURITY AWARENESS CHECKLIST

Check for clues.
- Links / Attachments
- Unfamiliar Sender
- Unexpected Email
- Errors
- Familiar, yet Unusual
- Personal Topics

Beware of tactics.
- Urgency
- Loss
- Authority
- Familiarity
- Reciprocation
- Popularity

Respond appropriately.
- Not sure? Navigate on your own, do some research, or ask the contact through another method.
- Sure? Mark as junk, block, and delete.
- Clicked? Report it immediately. Clicking was a mistake, but hiding it is willful harm to the company.

Thank you!
Falling for a phishing attack can harm the company's reputation, financials, systems, and hinder our ability to serve our clients. We appreciate your help and dedication!

CLUES

Clues are things which are clearly wrong with the email.

Links and Attachments
Are you being asked to click a link or open an attachment? Does hovering over the links show the expected destination URL?

Errors
Is the message unprofessional or covered with typos and grammatical errors?

Unfamiliar Sender
Do you recognize the name and email address of the sender? Is the domain similar, but not quite right?

Familiar, yet Unusual
Is your contact using an unusual salutation, tone, signature, or sending at a strange time of day?

Unexpected Email
Is this email "out of the blue," or is it a "follow up" on a request you did not make?

Personal Topics
Is the message of a personal nature (e.g., taxes, shipping, appointments, etc.)? Do you use your work email for personal communications?

TACTICS

Tactics are distractions to make you act without thinking.

Urgency
Phrases like "required" and "today" are designed to make you rush.

Loss
Language about losing access to something is designed to make you worry.

Authority
Posing as your boss, HR, or other authoritative group is designed to make you blindly obey.

Familiarity
Using publicly available information about you is designed to make you assume familiarity.

Reciprocation
Offering you something is designed to make you feel obligated to give something in return.

Popularity
Language about other people doing something you're not is designed to make you feel wrong.

Tandem

Phishing Checklist

Tandem.App/PH-Checklist

KEYS CONFERENCE

22

KEYS CONFERENCE

Clues

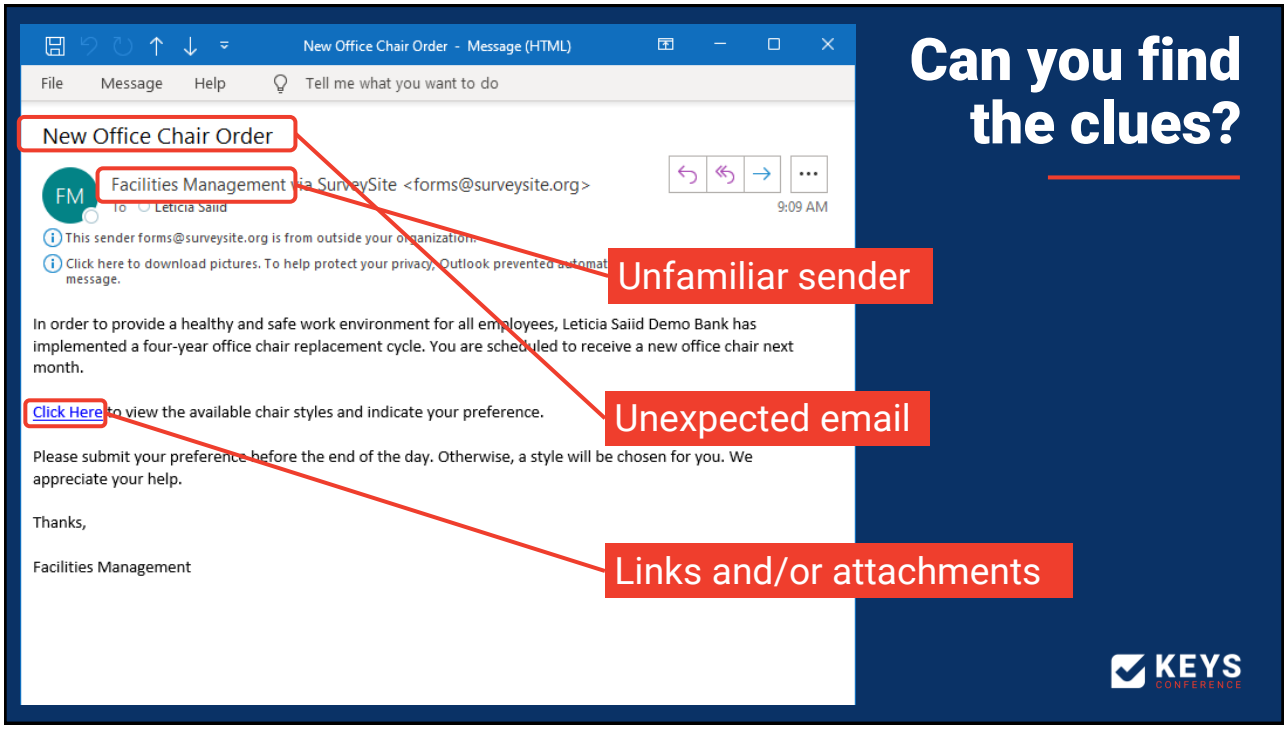
23

Phishing Clues

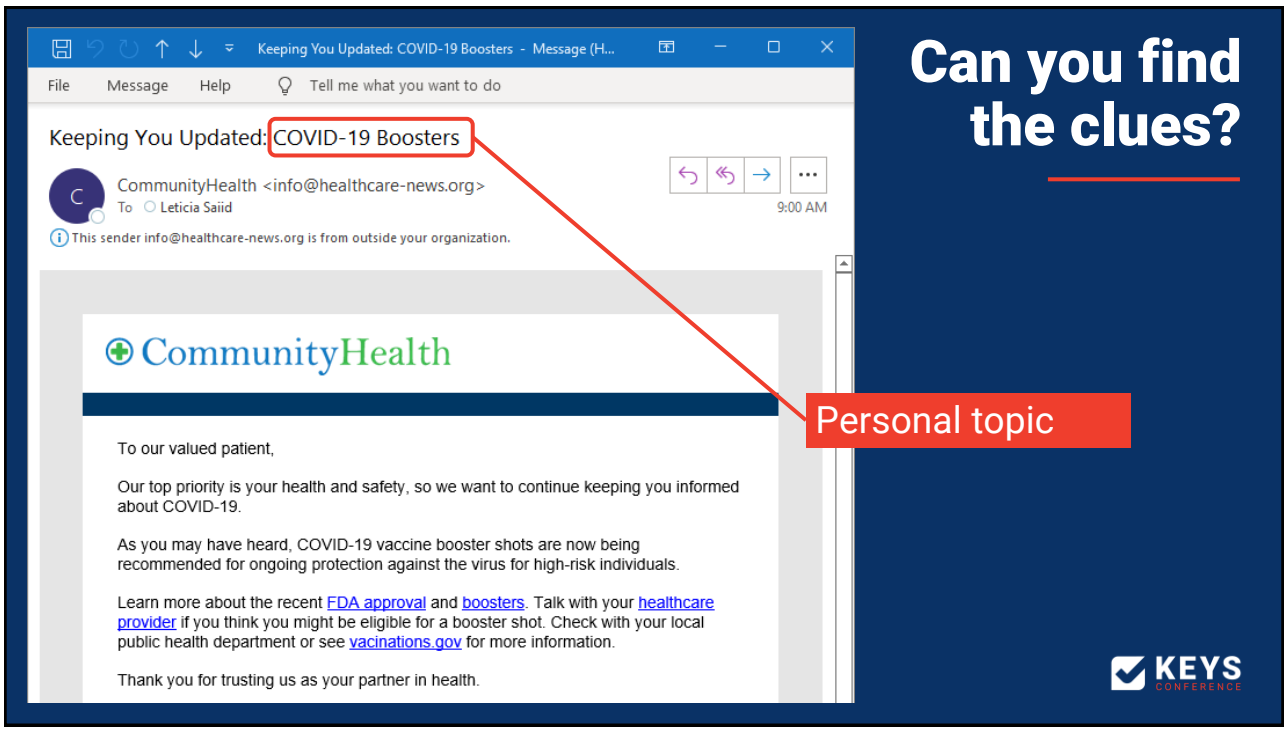
- Links and Attachments
- Unfamiliar Sender
- Unexpected Email
- Errors
- Familiar yet Unusual
- Personal Topic

KEYS CONFERENCE

24


New Office Chair Order - Message (HTML)
File
Message
Help
Tell me what you want to do
New Office Chair Order
FM
Facilities Management via SurveySite <forms@surveysite.org>
To Leticia Saiid
9:09 AM
This sender forms@surveysite.org is from outside your organization.
Click here to download pictures. To help protect your privacy, Outlook prevented automat
message.
In order to provide a healthy and safe work environment for all employees, Leticia Saiid Demo Bank has implemented a four-year office chair replacement cycle. You are scheduled to receive a new office chair next month.
Click Here to view the available chair styles and indicate your preference.
Please submit your preference before the end of the day. Otherwise, a style will be chosen for you. We appreciate your help.
Thanks,
Facilities Management
Can you find the clues?
Unfamiliar sender
Unexpected email
Links and/or attachments
KEYS
CONFERENCE

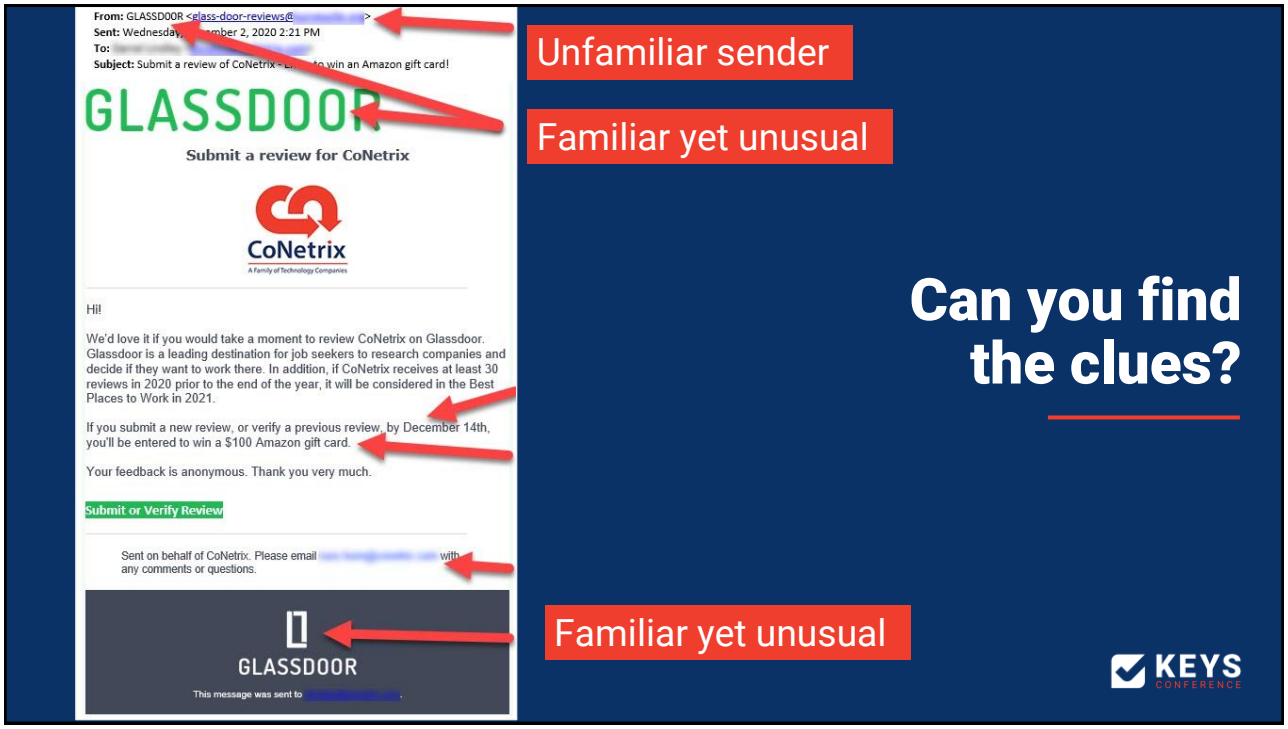
25


Keeping You Updated: COVID-19 Boosters - Message (H...
File
Message
Help
Tell me what you want to do
Keeping You Updated: COVID-19 Boosters
C
CommunityHealth <info@healthcare-news.org>
To Leticia Saiid
9:00 AM
This sender info@healthcare-news.org is from outside your organization.
CommunityHealth
To our valued patient,
Our top priority is your health and safety, so we want to continue keeping you informed about COVID-19.
As you may have heard, COVID-19 vaccine booster shots are now being recommended for ongoing protection against the virus for high-risk individuals.
Learn more about the recent FDA approval and boosters. Talk with your healthcare provider if you think you might be eligible for a booster shot. Check with your local public health department or see vacinations.gov for more information.
Thank you for trusting us as your partner in health.
Can you find the clues?
Personal topic
KEYS
CONFERENCE

26


Linked in
Leticia Saiid
Chief Of Staff at CoNetrix
1yr •
I failed a phishing test this past week. I don't fail these things. I always pass. I teach about this stuff!! Here were all my excuses as to why I messed. Excuses are the exact things phishers use to sneak by you.
1. I was in a hurry, aka, I was being lazy. It was my morning process of: delete the junk and take care of the easy stuff. This one looked like easy stuff. The email wasn't super clear, so I thought I would figure out what it needed from me after following the link.
2. It was from my boss. I didn't know exactly what it was or why. But it was from Russ, so I knew I wanted to help him take care of whatever thing he was trying to make happen that morning.
Looking at it now, it is riddled with issues and common tactics (see my image). I was just in too big of a hurry to see it. Lesson learned: SLOW DOWN.
KEYS CONFERENCE

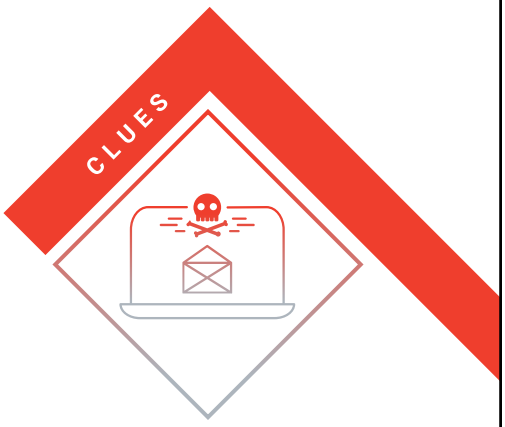
27


From: GLASSDOOR
Sent: Wednesday, December 2, 2020 2:21 PM
Subject: Submit a review of CoNetrix to win an Amazon gift card!
GLASSDOOR
Submit a review for CoNetrix
CoNetrix
Hi!
We'd love it if you would take a moment to review CoNetrix on Glassdoor. Glassdoor is a leading destination for job seekers to research companies and decide if they want to work there. In addition, if CoNetrix receives at least 30 reviews in 2020 prior to the end of the year, it will be considered in the Best Places to Work in 2021.
If you submit a new review, or verify a previous review, by December 14th, you'll be entered to win a $100 Amazon gift card.
Your feedback is anonymous. Thank you very much.
Submit or Verify Review
Sent on behalf of CoNetrix. Please email with any comments or questions.
GLASSDOOR
This message was sent to
Unfamiliar sender
Familiar yet unusual
Can you find the clues?
Familiar yet unusual
KEYS CONFERENCE

28

Phishing Clues

- Links and Attachments
- Unfamiliar Sender
- Unexpected Email
- Errors
- Familiar yet Unusual
- Personal Topic



KEYS CONFERENCE

29

KEYS CONFERENCE

Tactics

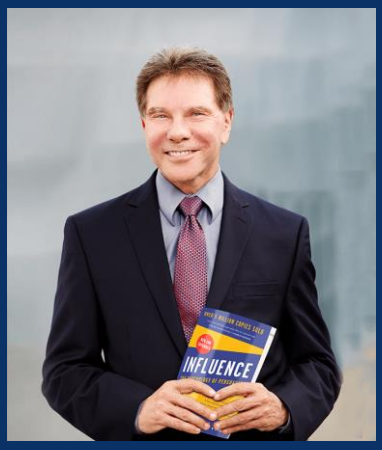
30

Phishing Tactics

Urgency
Loss
Reciprocation
Authority
Familiarity
Popularity

KEYS CONFERENCE

31



https://youtu.be/cFdCzN7RYbw

Influence: The Psychology of Persuasion

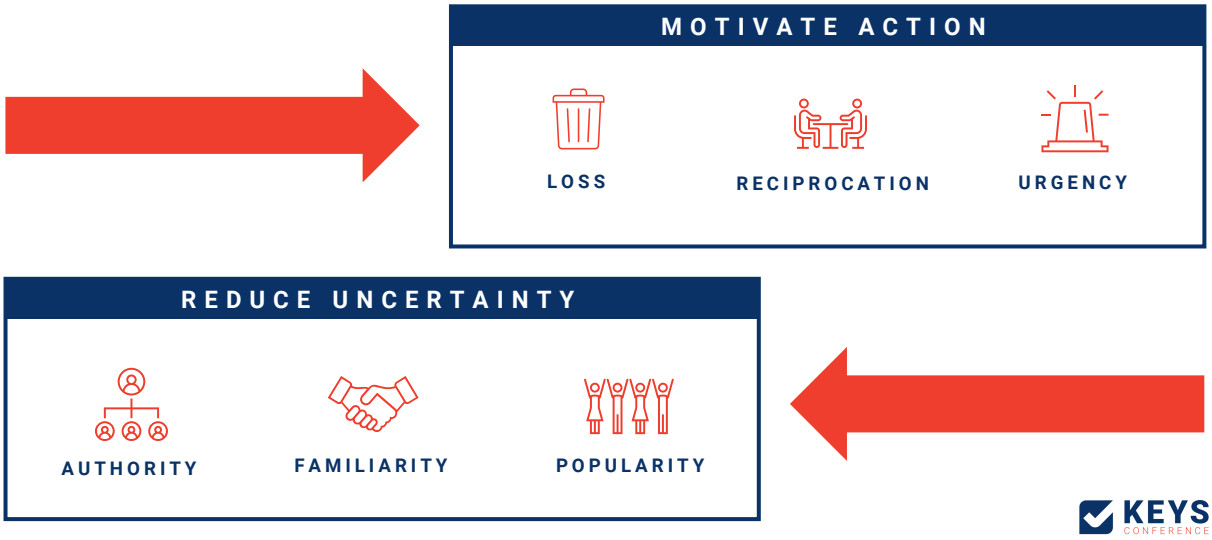
2006, UPDATED 2021

DR. ROBERT B. CIALDINI

KEYS CONFERENCE

32

Phishing Tactics Are Designed to:



33

"[Shortcuts] tell us when compliance with a request is likely to be correct and beneficial."

"The form and pace of modern life is not allowing us to make fully thoughtful decisions [...] Sometimes the issues may be so complicated, the time so tight, the distractions so intrusive, the emotional arousal so strong, or the mental fatigue so deep that we are in no cognitive condition to operate mindfully. Important topic or not, we have to take the shortcut."

NATURAL AUTOMATION

KEYS CONFERENCE

SOURCE: Influence - The Psychology of Persuasion by Dr. Robert Cialdini

34

LOSS

TO MOTIVATE ACTION

KEYS CONFERENCE

35

File Message Help Tell me what you want to do

New Office Chair Order

FM

Facilities Management via SurveySite <forms@surveysite.org>

To Leticia Saiid

9:09 AM

This sender forms@surveysite.org is from outside your organization.

Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

In order to provide a healthy and safe work environment for all employees, Leticia Saiid Demo Bank has implemented a four-year office chair replacement cycle. You are scheduled to receive a new office chair next month.

Click Here to view the available chair styles and indicate your preference.

Please submit your preference before the end of the day. Otherwise, a style will be chosen for you. We appreciate your help.

Thanks,

Facilities Management

LOSS

TO MOTIVATE ACTION

KEYS CONFERENCE

36

URGENCY

TO MOTIVATE ACTION

KEYS CONFERENCE

37

File Message Help Tell me what you want to do

New Office Chair Order

FM

Facilities Management via SurveySite <forms@surveysite.org>

To Leticia Saiid

9:09 AM

This sender forms@surveysite.org is from outside your organization.

Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

In order to provide a healthy and safe work environment for all employees, Leticia Saiid Demo Bank has implemented a four-year office chair replacement cycle. You are scheduled to receive a new office chair next month.

Click Here to view the available chair styles and indicate your preference.

Please submit your preference before the end of the day. Otherwise, a style will be chosen for you. We appreciate your help.

Thanks,

Facilities Management

URGENCY

TO MOTIVATE ACTION

KEYS CONFERENCE

38

RECIPROCATION

TO MOTIVATE ACTION

KEYS CONFERENCE

39

File Message Help Tell me what you want to do

New Office Chair Order

FM

Facilities Management via SurveySite <forms@surveysite.org>

To Leticia Saiid

9:09 AM

This sender forms@surveysite.org is from outside your organization.

Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

In order to provide a healthy and safe work environment for all employees, Leticia Saiid Demo Bank has implemented a four-year office chair replacement cycle. You are scheduled to receive a new office chair next month.

Click Here to view the available chair styles and indicate your preference.

Please submit your preference before the end of the day. Otherwise, a style will be chosen for you. We appreciate your help.

Thanks,

Facilities Management

RECIPROCATION

TO MOTIVATE ACTION

KEYS CONFERENCE

40

AUTHORITY

TO REDUCE UNCERTAINTY

KEYS CONFERENCE

41

File Message Help Tell me what you want to do

Signature needed - Please review COVID related changes to remote work policy

D director@bankcompliance.us
To Leticia Saiid 9:01 AM

This sender director@bankcompliance.us is from outside your organization.

Remote Work Policy Update.xlsx
10 KB

Dear Leticia Saiid,

We are updating our remote work policy due to changes in Federal COVID Protocols. Since these changes will affect almost all individuals associated with our company, we are requiring each employee to review the attached document and digitally sign that you have received this notice.

Remote Work Policy Update

Enforcement of the new policy updates will occur 5 business days from the date of this email. Please view and sign the document as soon as possible.

Thank you for your cooperation,
HR Management

AUTHORITY
REDUCE UNCERTAINTY

KEYS CONFERENCE

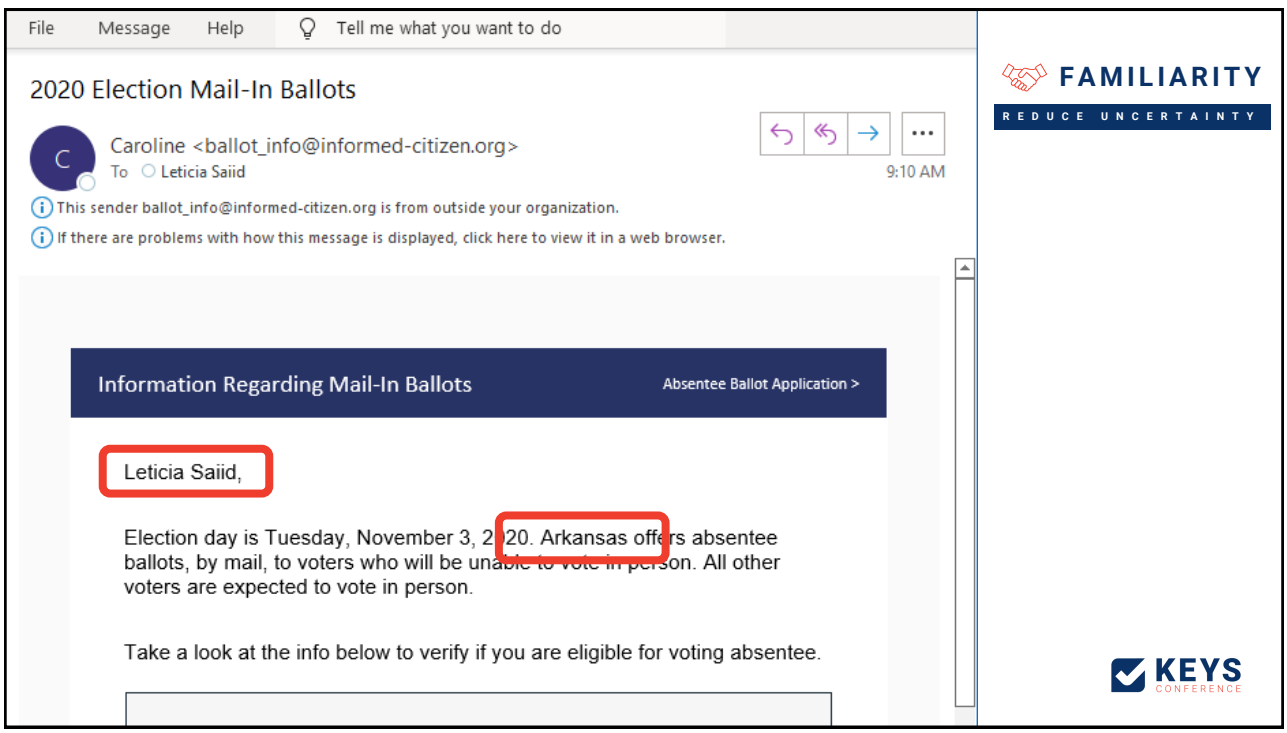
42

FAMILIARITY

TO REDUCE UNCERTAINTY

KEYS CONFERENCE

43



44

POPULARITY

TO REDUCE UNCERTAINTY

KEYS CONFERENCE

45

Social Conformity – Brain Games
https://www.youtube.com/watch?v=o8BkzvP19v4

KEYS CONFERENCE

46

To: Leticia Salid <lsalid@CoNetrix.com>
Subject: FW: Can you unsubscribe?

Hi Leticia,

The IT group found a way to unsubscribe from these obnoxious emails. Fill out the form on this site to unsubscribe your email address: http://www.onlineorders.co/email-lists/unsubscribe

Hope this helps.

- Jim

From: Alex Smith (alex.smith@communitybanks.us)
Sent: 06/15/2021 7:52 AM
To: Jim Walsh (james.walsh@communitybanks.us)
Subject: RE: Can you unsubscribe?

Jim,

It looks like they do have a link to unsubscribe, but it's really hidden on they're site. Here you go: http://www.onlineorders.co/email-lists/unsubscribe

Thanks!

Alex Smith
IT Department

POPULARITY
REDUCE UNCERTAINTY

KEYS CONFERENCE

47

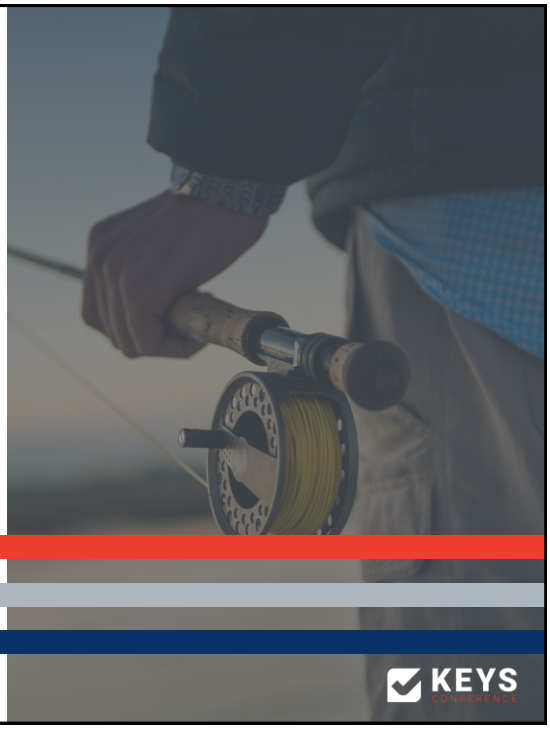
Phishing Tactics

Urgency
Loss
Reciprocation
Authority
Familiarity
Popularity

KEYS CONFERENCE

48

Preparing for Phishing



KEYS CONFERENCE

49

Phishing Checklist

CHECKLIST INSTRUCTIONS

Fold or cut the quick checklist on the right. Place it somewhere you can see when reading your emails. Read the rest of this document to better understand each checklist item.

RESPONSES

Not sure if it is phishing?
Navigate to the information on your own. Any legitimate company will have a way outside of clicking an email link. -OR- Search online for more information to support your choice to click or ignore. -OR- Contact the sender (if trusted) through another method (e.g., phone call, text message, etc.) to verify before clicking.

Are you sure it's phishing?
Mark the message as junk, block the sender email address, and permanently delete the message.

Did you click a phishing link?
Report it to ISD/IT immediately. Clicking was a mistake, hiding it is willful harm to the company.

MY PHISHING SECURITY AWARENESS CHECKLIST

Check for clues.
- Links / Attachments
- Unfamiliar Sender
- Unexpected Email
- Errors
- Familiar, yet Unusual
- Personal Topics

Beware of tactics.
- Urgency
- Loss
- Authority
- Familiarity
- Reciprocation
- Popularity

Respond appropriately.
- Not sure? Navigate on your own, do some research, or ask the contact through another method.
- Sure? Mark as junk, block, and delete.
- Clicked? Report it immediately. Clicking was a mistake, but hiding it is willful harm to the company.

Thank you!
Falling for a phishing attack can harm the company's reputation, financials, systems, and hinder our ability to serve our clients. We appreciate your help and dedication!

CLUES

Clues are things which are clearly wrong with the email.

Links and Attachments
Are you being asked to click a link or open an attachment? Does hovering over the links show the expected destination URL?

Errors
Is the message unprofessional or covered with typos and grammatical errors?

Unfamiliar Sender
Do you recognize the name and email address of the sender? Is the domain similar, but not quite right?

Familiar, yet Unusual
Is your contact using an unusual salutation, tone, signature, or sending at a strange time of day?

Unexpected Email
Is this email "out of the blue," or is it a "follow up" on a request you did not make?

Personal Topics
Is the message of a personal nature (e.g., taxes, shipping, appointments, etc.)? Do you use your work email for personal communications?

TACTICS

Tactics are distractions to make you act without thinking.

Urgency
Phrases like "required" and "today" are designed to make you rush.

Loss
Language about losing access to something is designed to make you worry.

Authority
Posing as your boss, HR, or other authoritative group is designed to make you blindly obey.

Familiarity
Using publicly available information about you is designed to make you assume familiarity.

Reciprocation
Offering you something is designed to make you feel obligated to give something in return.

Popularity
Language about other people doing something you're not is designed to make you feel wrong.

Tandem

Phishing Checklist

Tandem.App/PH-Checklist

BOOK RECOMMENDATION
The Checklist Manifesto

KEYS CONFERENCE

50

51

TIMELY AND SPECIFIC FEEDBACK

From: John Doe <jdoe@tandem.com> — Unfamiliar sender
Sent: Tuesday, March 29th, 2022 8:00 AM
To: Leticia Saiid <lsaiid@conetrix.com>
Subject: FWD: From Tandem Conference — Unexpected Email

Familiarity

Hello valued attendee, — Familiar but unusual

I hope you are as excited for the event as I am.

Errors

Reciprocation

Here is a copy of your event registration… Pls review & fill out attached form BEFORE 12:00 TODAY. — Urgency

Reg0329.html (7KB) — Links & Attachments

KEYS CONFERENCE

52

Respond Appropriately

NOT SURE?

- Navigate on your own.
- Do some research.
- Confirm with the sender via another method.

CERTAIN?

- Mark as "Junk."
- Block the sender.
- Permanently delete.
- Contact IT.

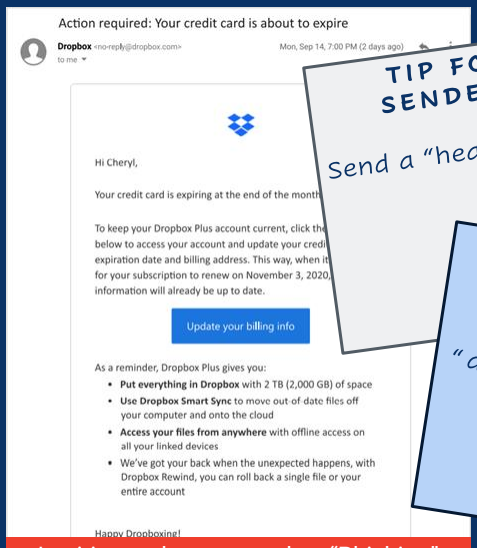
CLICKED?

Report it to IT immediately.

KEYS CONFERENCE

53

GREATHORN STUDY



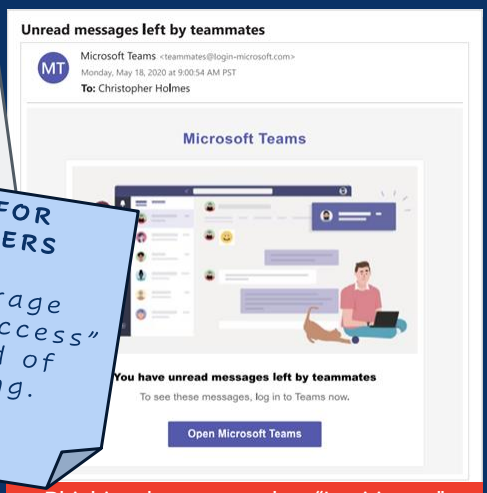
Legitimate, but reported as "Phishing" **55%** of the time.

TIP FOR SENDERS

Send a "heads-up."

TIP FOR SENDERS

Encourage "direct access" instead of clicking.



Phishing, but reported as "Legitimate" **53%** of the time.

https://info.greathorn.com/report-2020-end-user-phishing-report/

KEYS CONFERENCE

54

Tandem™
Phishing

Learn More

55

Recap

WHAT WE COVERED

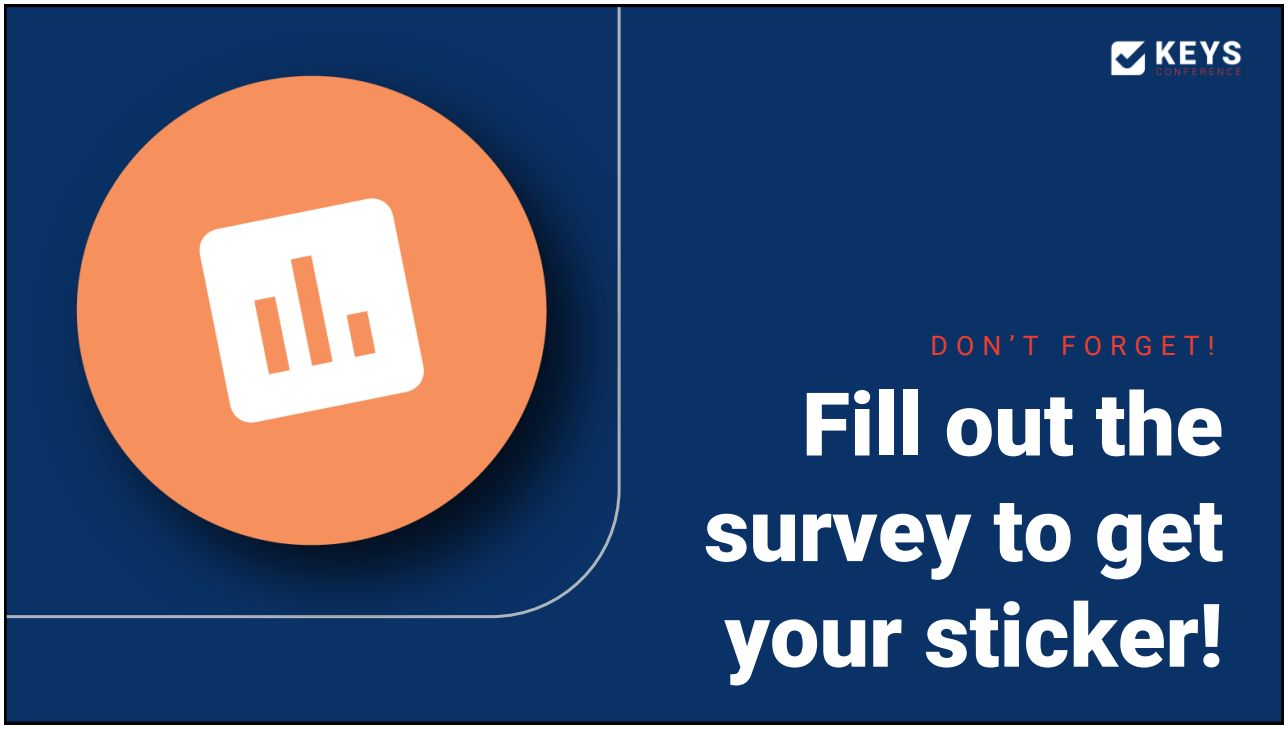
- What is phishing?
- What does effective phishing look like?
- Is there a better way to educate on phishing? C.A.T.C.H.
- Preparing for Phishing

?

ANY QUESTIONS?

KEYS CONFERENCE

56



57

Upcoming Sessions

TANDEM

So You're an Admin…

Cory Faust, Tandem

RISK & COMPLIANCE

CoNetrix Technology Engineers: A Panel Discussion

Rob Garrison, Brad Copeland, & Mike Richline, CoNetrix Technology

CYBERSECURITY

Better Your Communication Between Technical & Non-Technical People

Brad Landis & Brian Whipple, Tandem

KEYS CONFERENCE

58