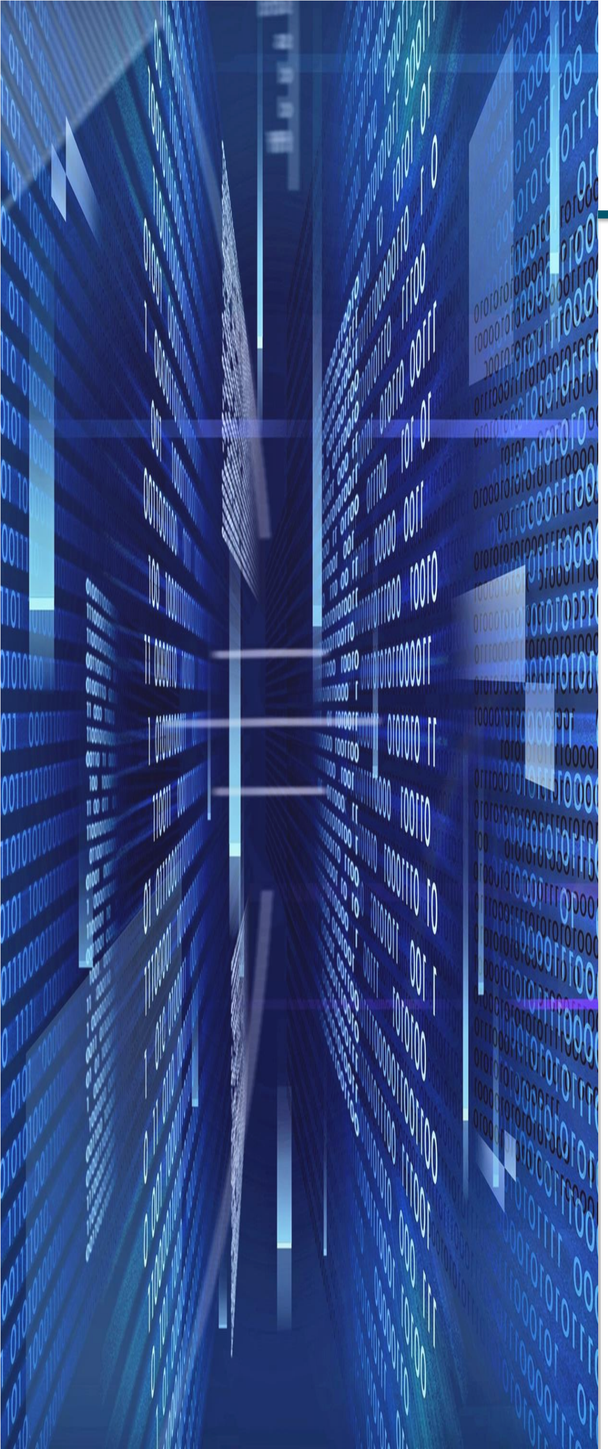


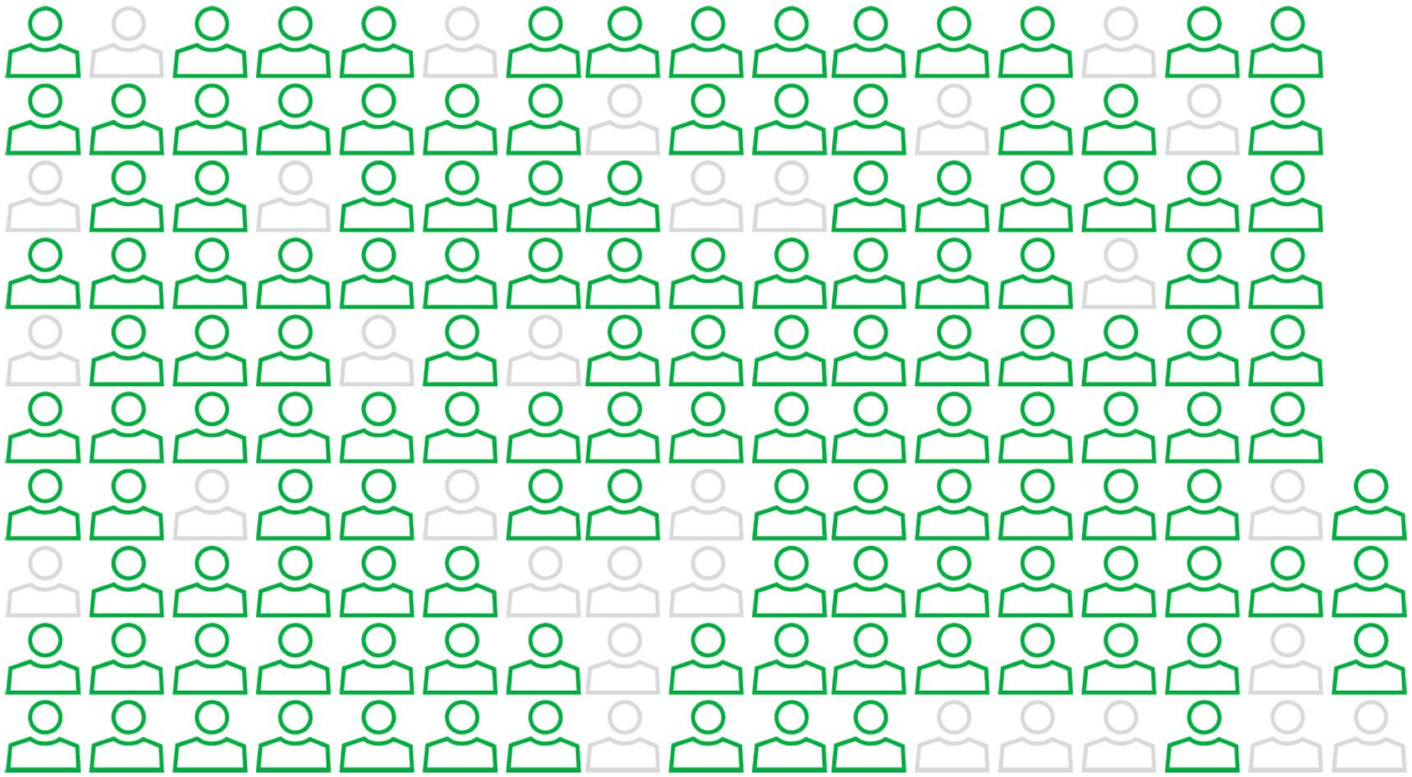
Social Engineering

Prof. Federica Paci

Lecture Outline

- What is social engineering?
- Who is behind social engineering attacks
- Social engineering attack lifecycle
- Types of social engineering attacks
- Phishing Attacks
  - How to identify a phishing email
  - Influence Tactics
  - How to identify a phishing website
- How to prevent phishing attacks

Social engineering attacks are on the rise



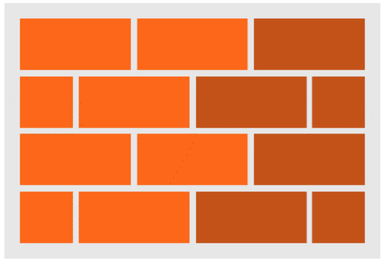
The human element continues to drive breaches. This year 82% of breaches involved the human element. Whether it is the Use of stolen credentials, Phishing, Misuse, or simply an Error, people continue to play a very large role in incidents and breaches alike.

What is social engineering?

What is social engineering?

Psychological manipulation of people into performing actions or divulgating personal information

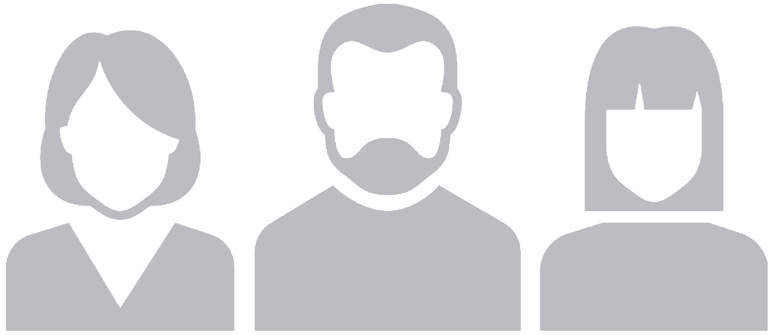
The Soft Center in Hard Shell



Firewalls

Access Controls

Anti Virus



…vulnerable humans

“A company can spend hundreds of thousands of dollars on firewalls, intrusion detection systems and encryption and other security technologies, but if an attacker can call one trusted person within the company, and that person complies, and if the attacker gets in, then all that money spent in technology is essentially wasted”, Kevin Mitnick

Who is behind social engineering attacks?

- Cybercriminals
  - Conduct financial heist, ransomware attacks or DDoS attacks
- Identity Thieves
  - use stolen personally identifiable information for their own purpose, and then either sell it on the dark web or post it online for all to see
- Scam Artists
  - engage in fraudulent or deceptive actions to defraud others
  - Examples: romance scams, facebook lottery scam, bank and financial accounts schemes

Lazarus Group: Bangladesh's Bank Financial Heist

How a hacker's typo helped stop a billion dollar bank heist

By Serajul Quadir

6 MIN READ

DHAKA (Reuters) - A spelling mistake in an online bank transfer instruction helped prevent a nearly $1 billion heist last month involving the Bangladesh central bank and the New York Federal Reserve, banking officials said.

President Macron's Identity Theft

Two Frenchmen on trial for stealing President Macron's online identity

The main defendant is accused of using a Gmail address purporting to belong to Macron to send a long political email titled "10 good reasons not to vote for me."

WORLD Updated: Mar 14, 2018, 17:01 IST

Associated Press
Associated Press, Paris

Facebook Lottery Scam

'Jennifer Goosen':

Oh i see.. I am delighted to inform you that your name was luckily selected among the 10 lucky winners who won the sum of $50,000.00 on the Facebook online lottery international draw. NOTE:this is 100% real and legit and the FBI are aware of this lottery promo.. You can also check this link to find the best history of the Facebook past winners: (spammy link containing the words 'winners' and 'Facebook').

Attack Life Cycle

Information Gathering

Establish Relationships

Exploitation

Execution

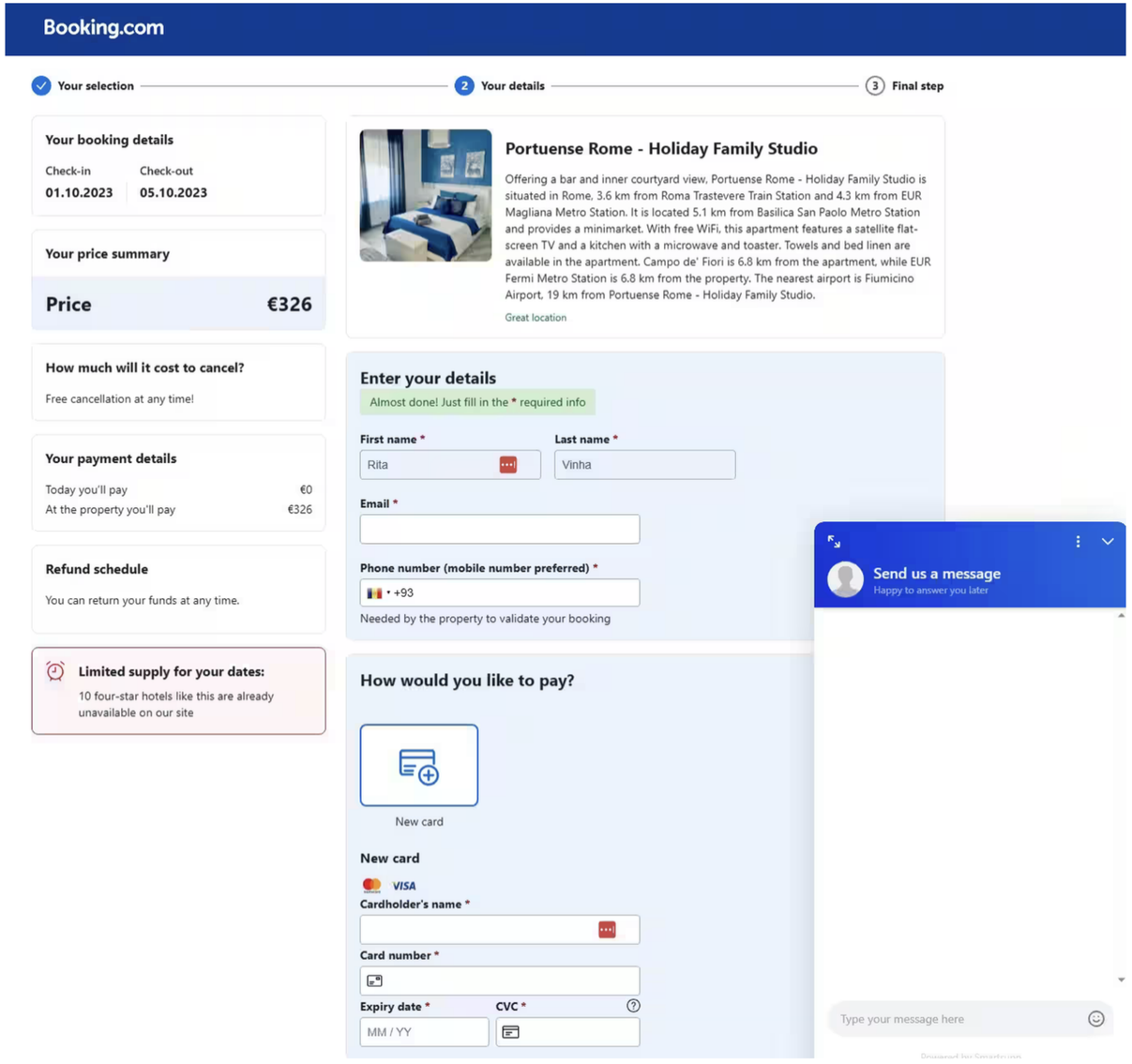
Types of Social Engineering Attacks

- Phishing
- Spear phishing
- Whaling
- Vishing
- SMiShing
- Dumpster Diving
- Shoulder Surfing
- Tailgating

Phishing

Phishing is the attempt to acquire sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money), often for malicious reasons, by masquerading as a trustworthy entity in an electronic communication

Phishing



Dear Valued Guest,

Due to an update of the booking rules, we are forced to request an additional card confirmation to guarantee your arrival. This procedure will take no more than 5 minutes. You have 24 hours to confirm your reservation, otherwise it will be cancelled by the booking system itself.

Please, follow the personal link: https://booking.guest-approve.info/reservation/606667156

IMPORTANT!
Prior to commencing the verification process, we kindly request that you review the limits set by your bank and ensure that your card balance is sufficient to cover the equivalent amount of your reservation. Please be aware that a microtransaction will occur, deducting the total sum of your booking. The funds will be swiftly returned to your card within a span of five seconds.

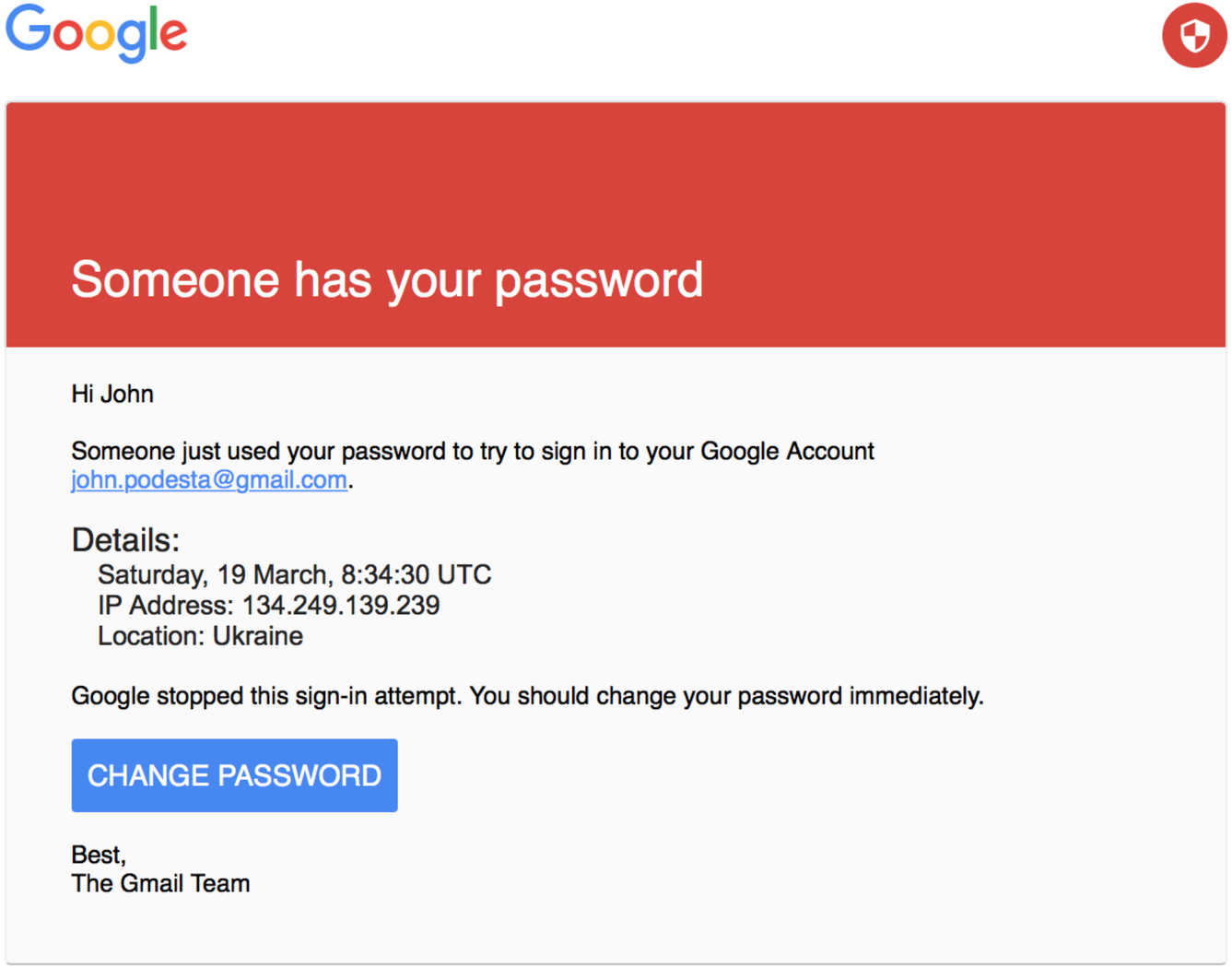
Best regards,

Grandi by Center Hotels

Spearphishing

A phishing attack specifically mounted against a target organization or user, frequently tailored to the victim by representing information that is unique to them in order to build authenticity

DNC – John Podesta spearphishing attack



Google

Someone has your password

Hi John

Someone just used your password to try to sign in to your Google Account john.podesta@gmail.com.

Details:
Saturday, 19 March, 8:34:30 UTC
IP Address: 134.249.139.239
Location: Ukraine

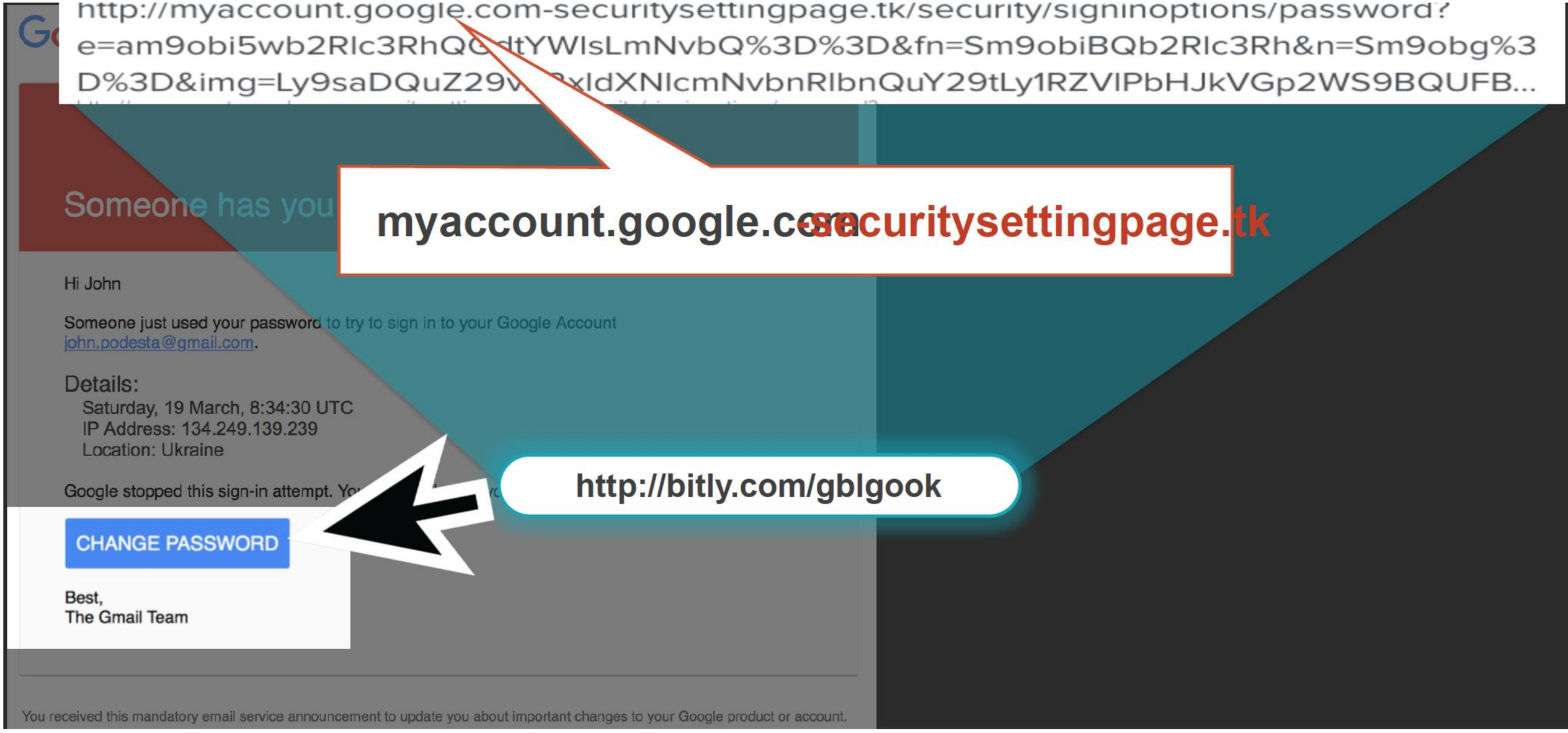
Google stopped this sign-in attempt. You should change your password immediately.

CHANGE PASSWORD

Best,
The Gmail Team

You received this mandatory email service announcement to update you about important changes to your Google product or account.

DNC – John Podesta spearphishing attack



Whaling

Chinese scammers take Mattel to the bank, Phishing them for $3 million

News

Mar 29, 2016 • 3 mins

Cybercrime | Security | Social Engineering

Thieves took advantage of a recent company shakeup and corporate policy regarding payments

Related content

Smishing

Retool Falls Victim to SMS-Based Phishing Attack Affecting 27 Cloud Clients

Sep 18, 2023 Newsroom Cyber Attack / Data Breach

Vishing

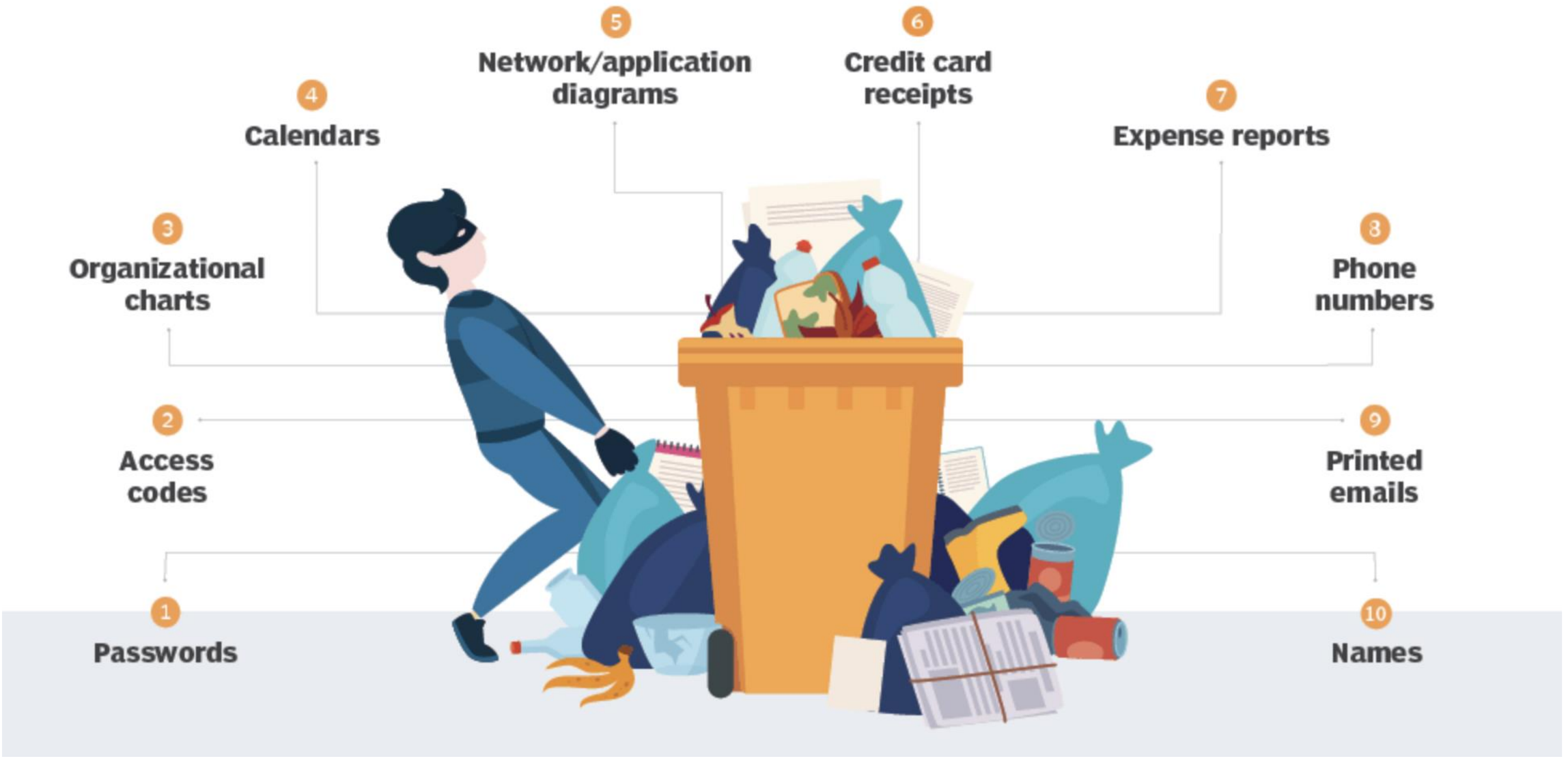
Cybercriminals use voice phishing to scam $243000 out of a UK Energy Firm

By iZOOlogic | January 2, 2020

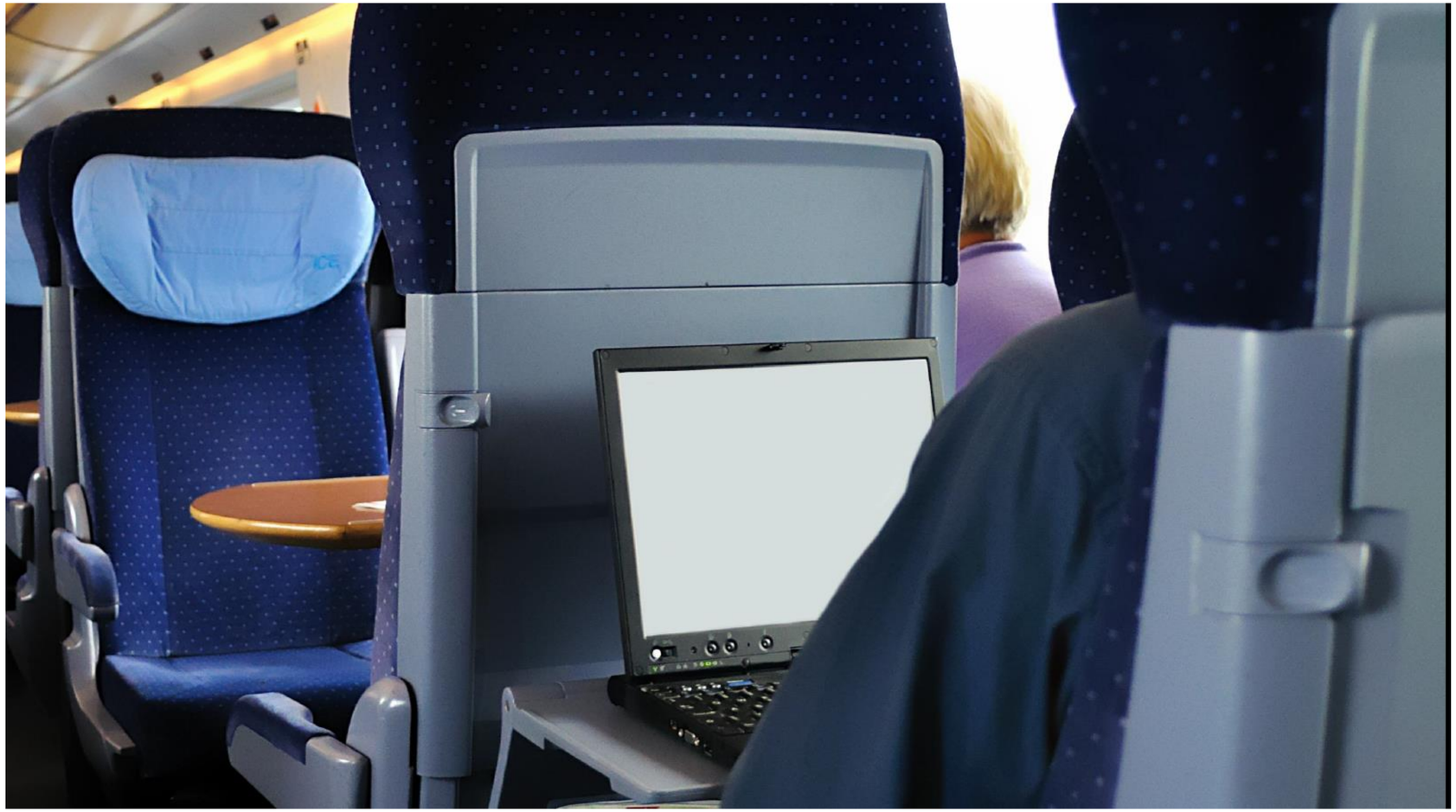
Categories

- Events (4)
- Industry (355)
  - Telecommunications (85)
  - Banking and Finance (233)
  - Airline (53)
  - Gaming (85)
- Region (1,033)
  - UK (210)
  - US (541)

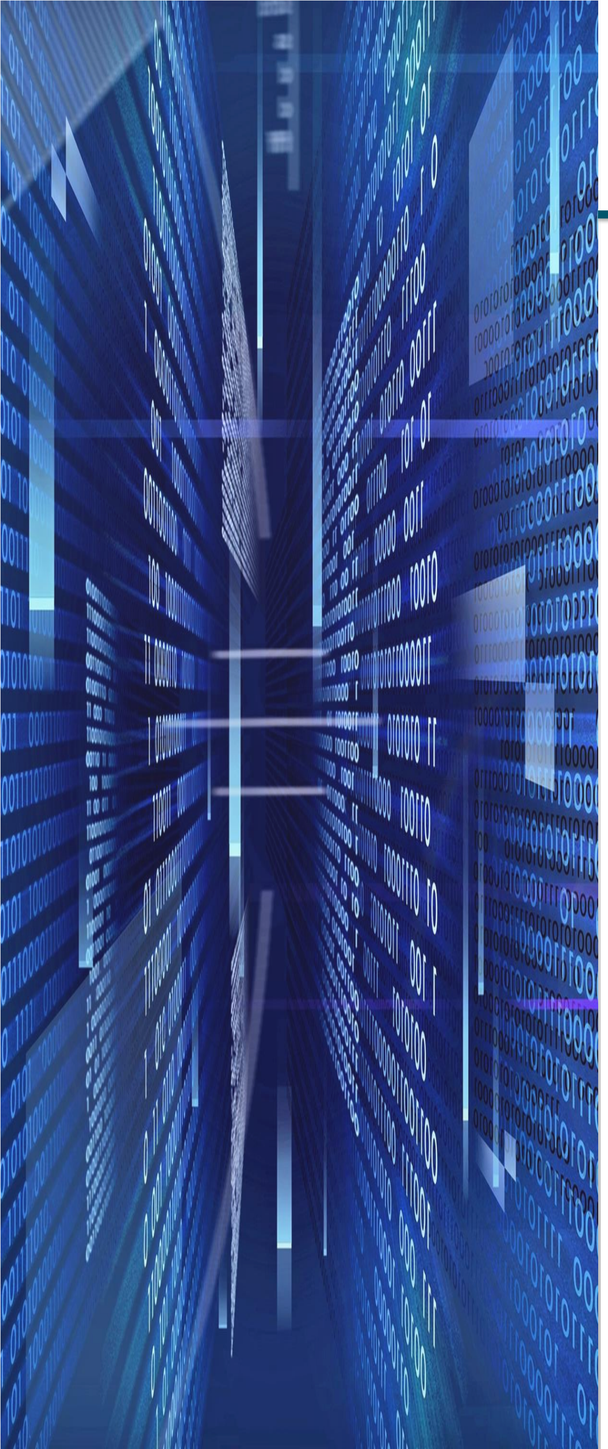
Dumpster Diving



Shoulder Surfing



Tailgating



Phishing Attacks

Prof. Federica Paci

How effective are phishing attacks?

88% of organizations around the world experienced spear phishing attempts in 2019

How effective are phishing attacks?

95% of all attacks on enterprise networks are the result of successful spear phishing

How effective are phishing attacks?

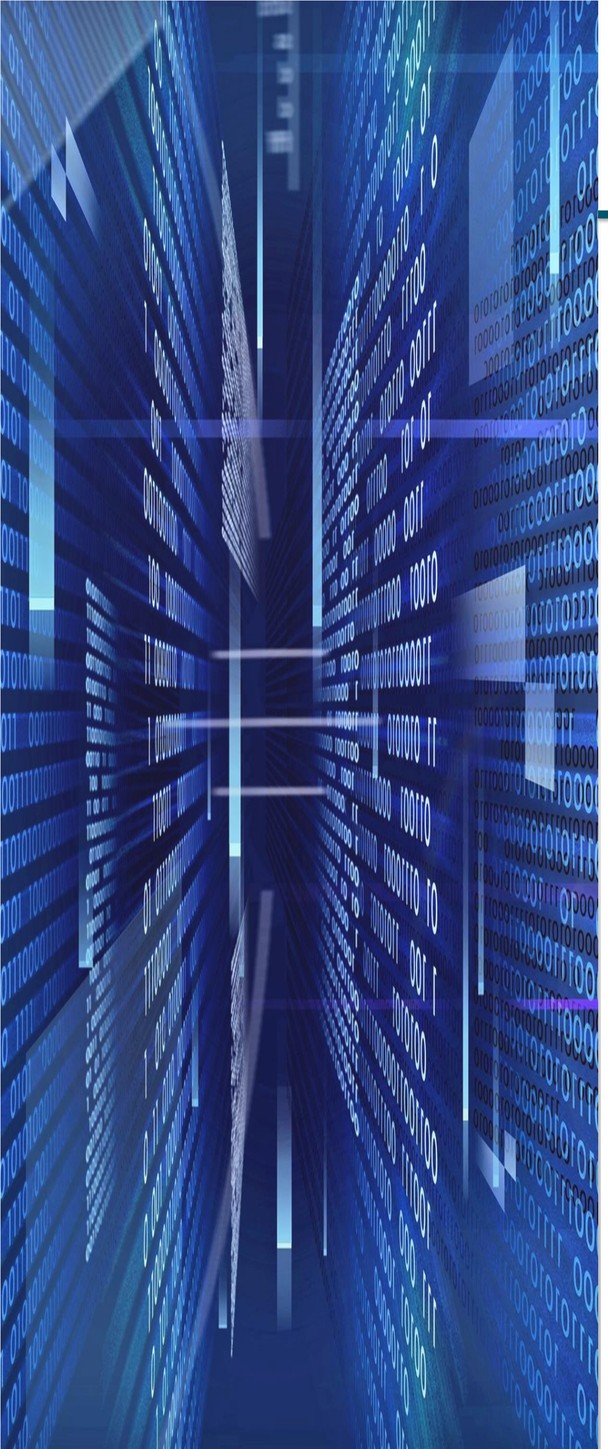
97% of users cannot identify a sophisticated phishing email

How effective are phishing attacks?

30% of the emails are opened by the target victims

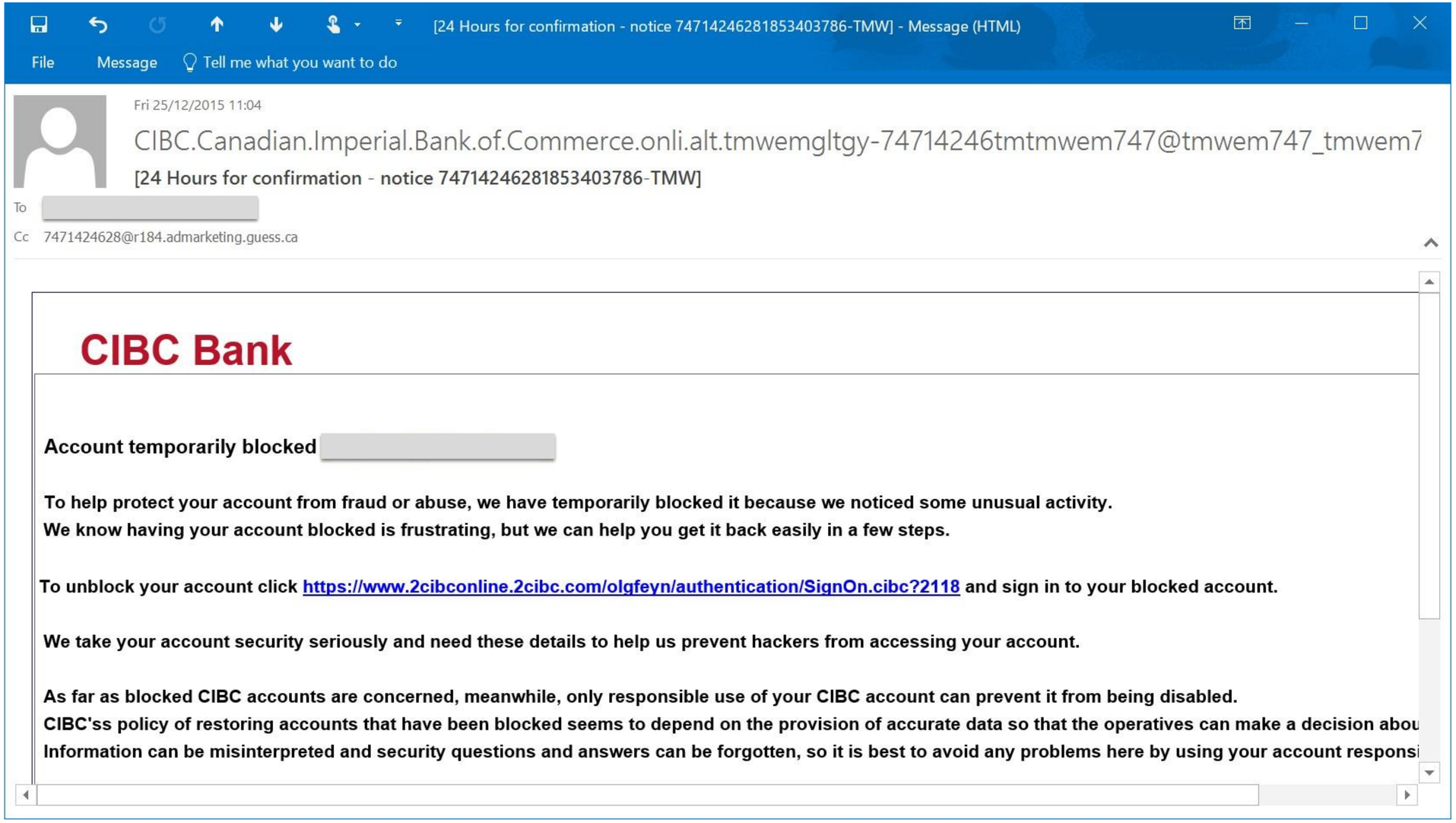
12% clicked on the link in the email or open the attachment

15% of victims are target at least one more time within the same year

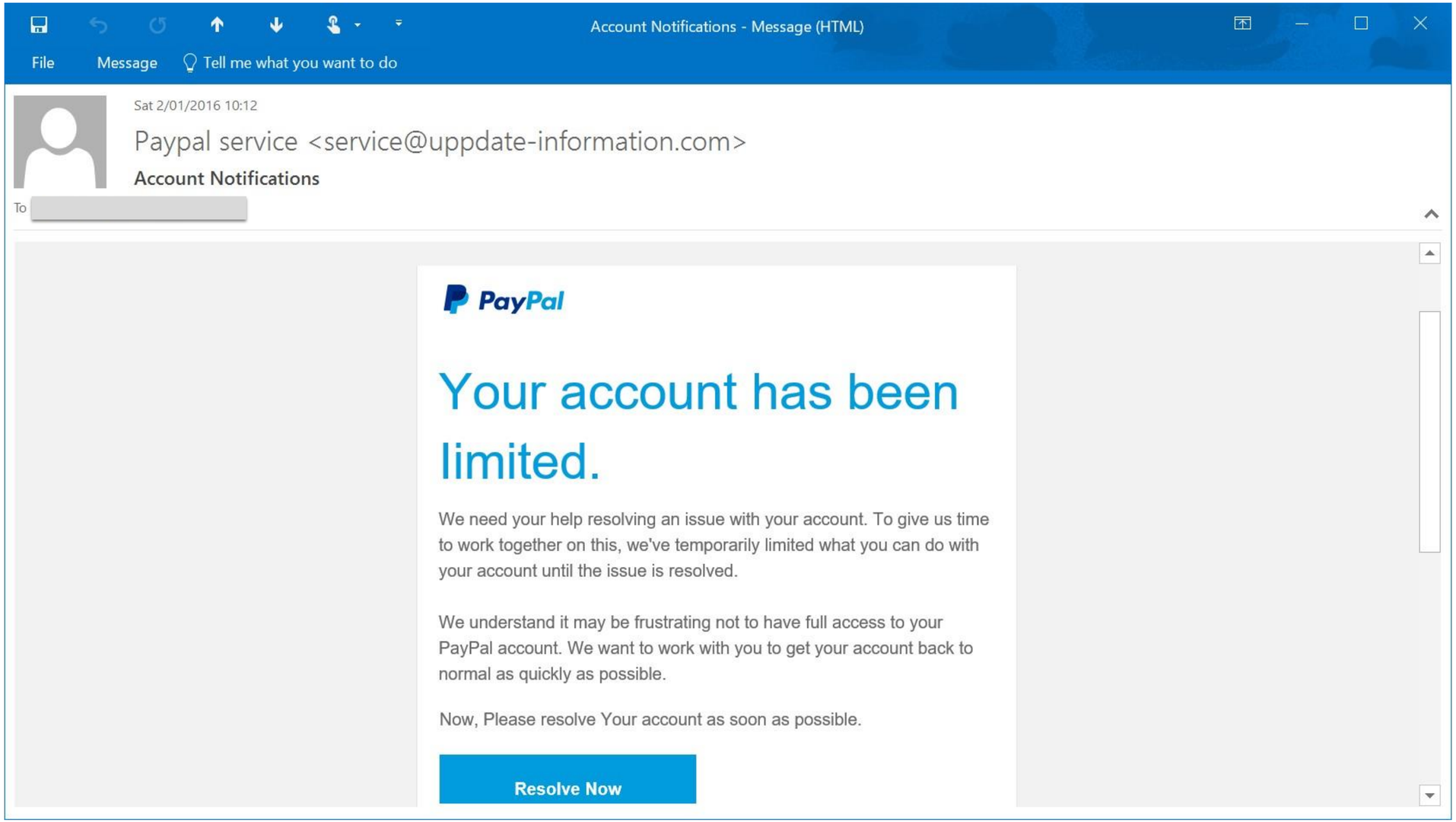


Phishing Emails

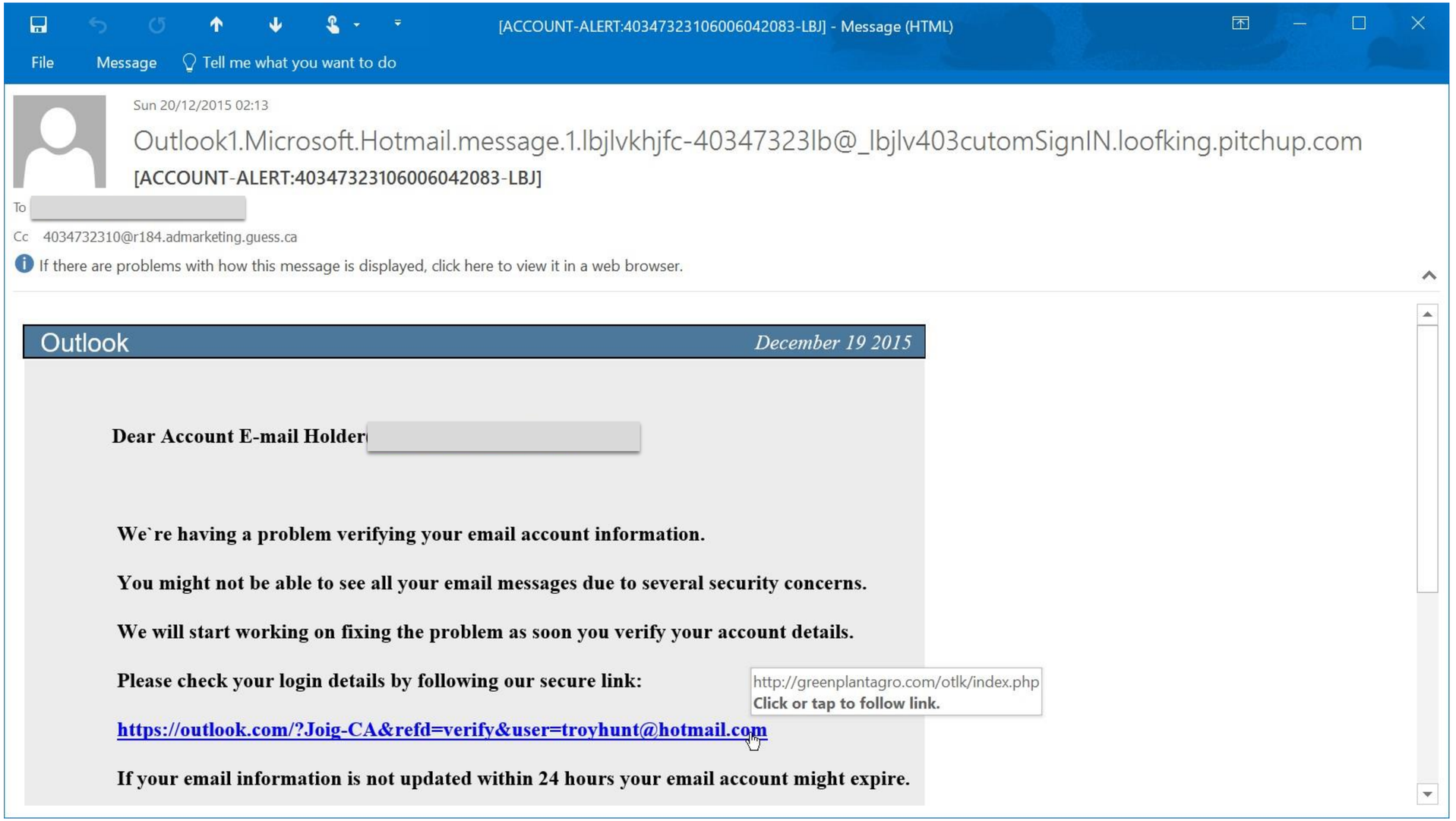
Branding Inconsistencies

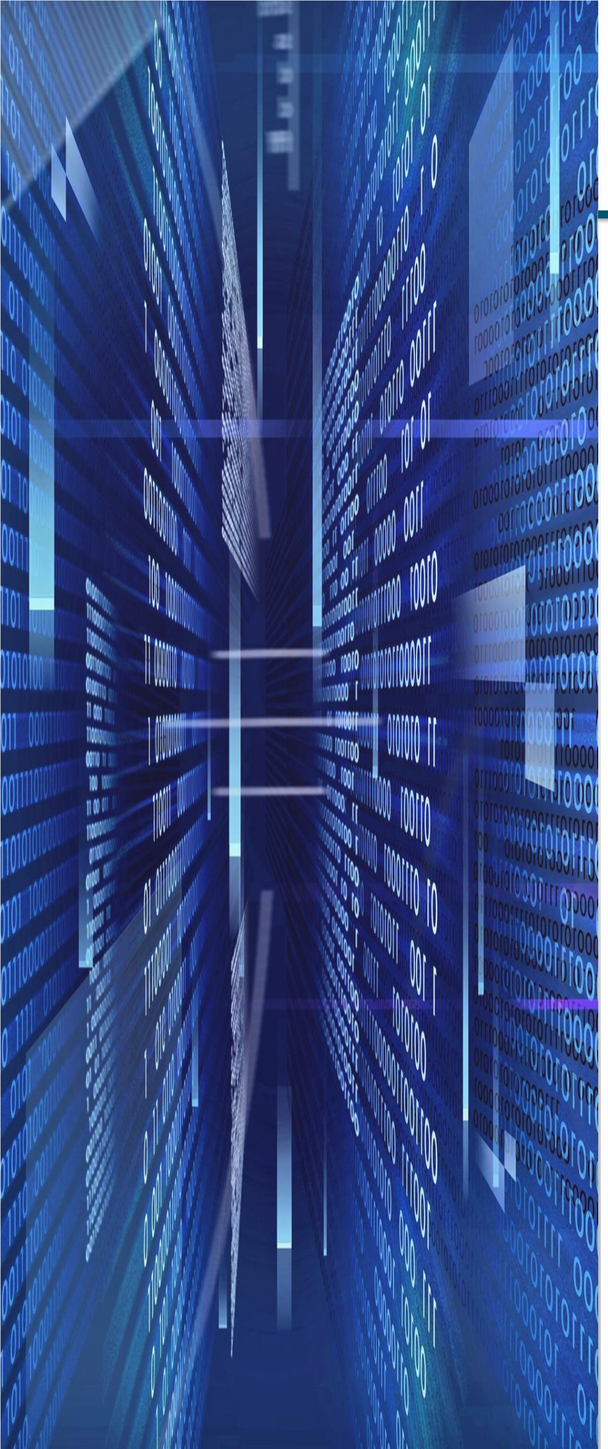


Sender and Cashier



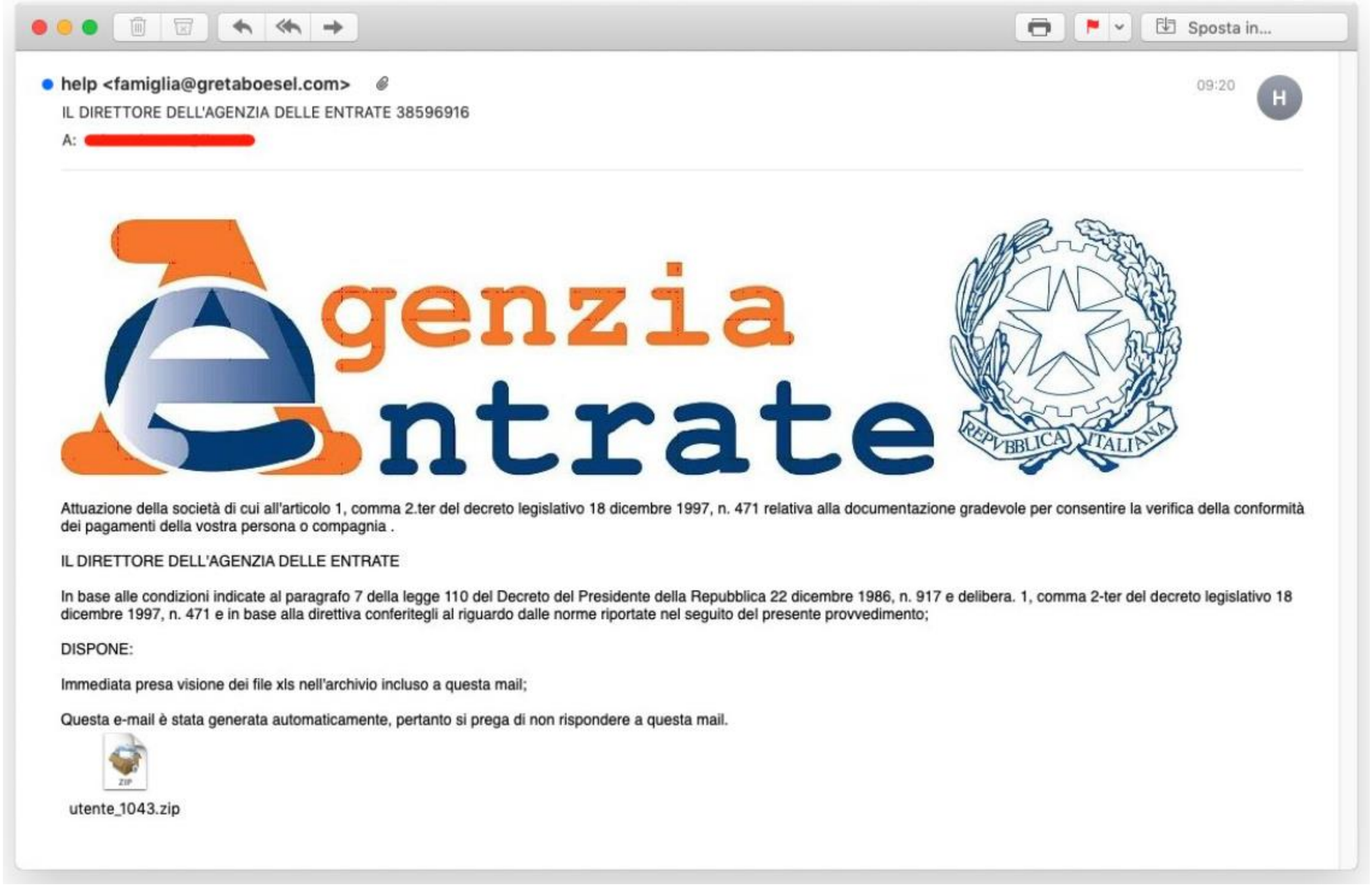
Hyperlink target mismatch





Influence Tactics

Exploiting Authority



help <famiglia@gretaboesel.com>

09:20

IL DIRETTORE DELL'AGENZIA DELLE ENTRATE 38596916

A: [redacted]

Attuazione della società di cui all'articolo 1, comma 2.ter del decreto legislativo 18 dicembre 1997, n. 471 relativa alla documentazione gradevole per consentire la verifica della conformità dei pagamenti della vostra persona o compagnia .

IL DIRETTORE DELL'AGENZIA DELLE ENTRATE

In base alle condizioni indicate al paragrafo 7 della legge 110 del Decreto del Presidente della Repubblica 22 dicembre 1986, n. 917 e delibera. 1, comma 2-ter del decreto legislativo 18 dicembre 1997, n. 471 e in base alla direttiva conferitegli al riguardo dalle norme riportate nel seguito del presente provvedimento;

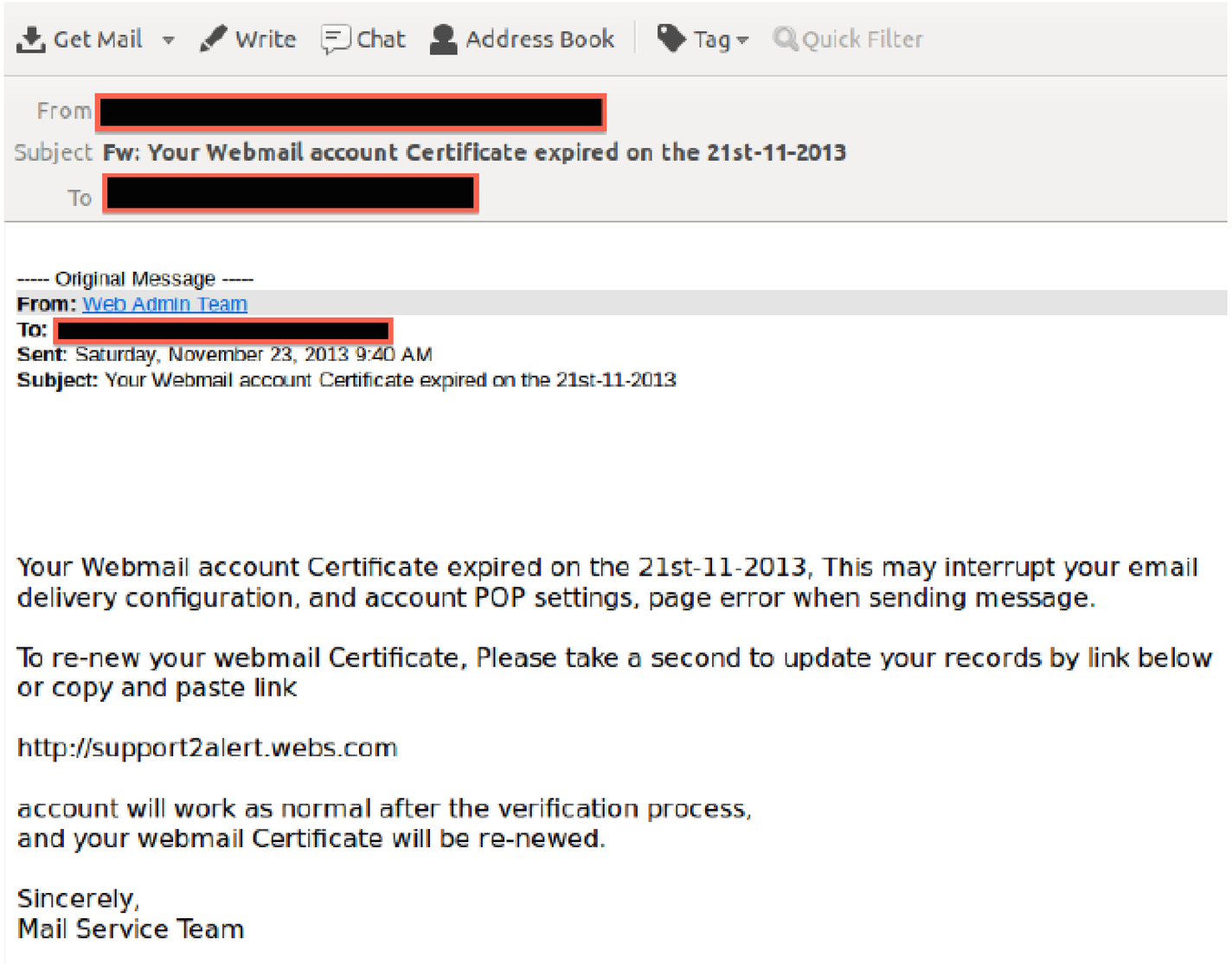
DISPONE:

Immediata presa visione dei file xls nell'archivio incluso a questa mail;

Questa e-mail è stata generata automaticamente, pertanto si prega di non rispondere a questa mail.

utente_1043.zip

Exploiting Scarcity



Get Mail | Write | Chat | Address Book | Tag | Quick Filter

From [redacted]

Subject **Fw: Your Webmail account Certificate expired on the 21st-11-2013**

To [redacted]

----- Original Message -----
From: Web Admin Team
To: [redacted]
Sent: Saturday, November 23, 2013 9:40 AM
Subject: Your Webmail account Certificate expired on the 21st-11-2013

Your Webmail account Certificate expired on the 21st-11-2013, This may interrupt your email delivery configuration, and account POP settings, page error when sending message.

To re-new your webmail Certificate, Please take a second to update your records by link below or copy and paste link

http://support2alert.webs.com

account will work as normal after the verification process,
and your webmail Certificate will be re-newed.

Sincerely,
Mail Service Team

Exploiting Commitment

----- Original Message -----
From: Notice to Appear
To: [redacted]
Sent: Monday, December 23, 2013 5:47 PM
Subject: [!! SPAM] Suspicious part has been deleted : Notice of appearance in court NR#9386

Notice to Appear,

Hereby you are notified that you have been scheduled to appear for your hearing that
will take place in the court of Washington in January 14, 2014 at 10:00 am.

Please bring all documents and witnesses relating to this case with you to Court on your hearing date.

The copy of the court notice is attached to this letter.
Please, read it thoroughly.

Note: If you do not attend the hearing the judge may hear the case in your absence.

Yours truly,
Emily Smith
Clerk to the Court.

Exploiting Liking

Niets op mijn fb.pagina's hiervan terug te vinden. Phishing.

Groeten
[redacted]

Van: Facebook [mailto:notification+zrdohvri=vd1@facebookmail.com]
Verzonden: maandag 12 augustus 2013 23:51
Aan: [redacted]
Onderwerp: Lorie Fox tagged 4 photos of you on Facebook

facebook

Lorie Fox added 4 photos of you.

See photos | Go to notifications

This message was sent to [redacted] If you don't want to receive these emails from Facebook in the future, please click: unsubscribe.
Facebook, Inc. Attention: Department 415 P.O Box 10005 Palo Alto CA 94303

Exploiting Reciprocation

Congratulations, you have won $20 dollars towards your next purchase of edible goods. This money has been donated by APPLES Co., a non profit organization founded to promote the purchase of organic foods.

These $20 will be applicable in any local grocery supermarket.

You will receive it in the form a gift card that will be sent to your mailing address. In the meantime, please click the link below to vote for APPLES Co. as the top 10 non-profit of the year in our region! < link >”

Exploiting Social Proof

I would like to invite you to **join the thousands of other clients** who have experienced our vacation excursions. We are currently **serving ten clients in your** neighborhood and this is how we got your contact information.

Our company called Dunes was developed for clients to experience lavish vacation spots at an affordable price. We have earned the title of Top 10 Best Travel Agency from TripAdvisor.

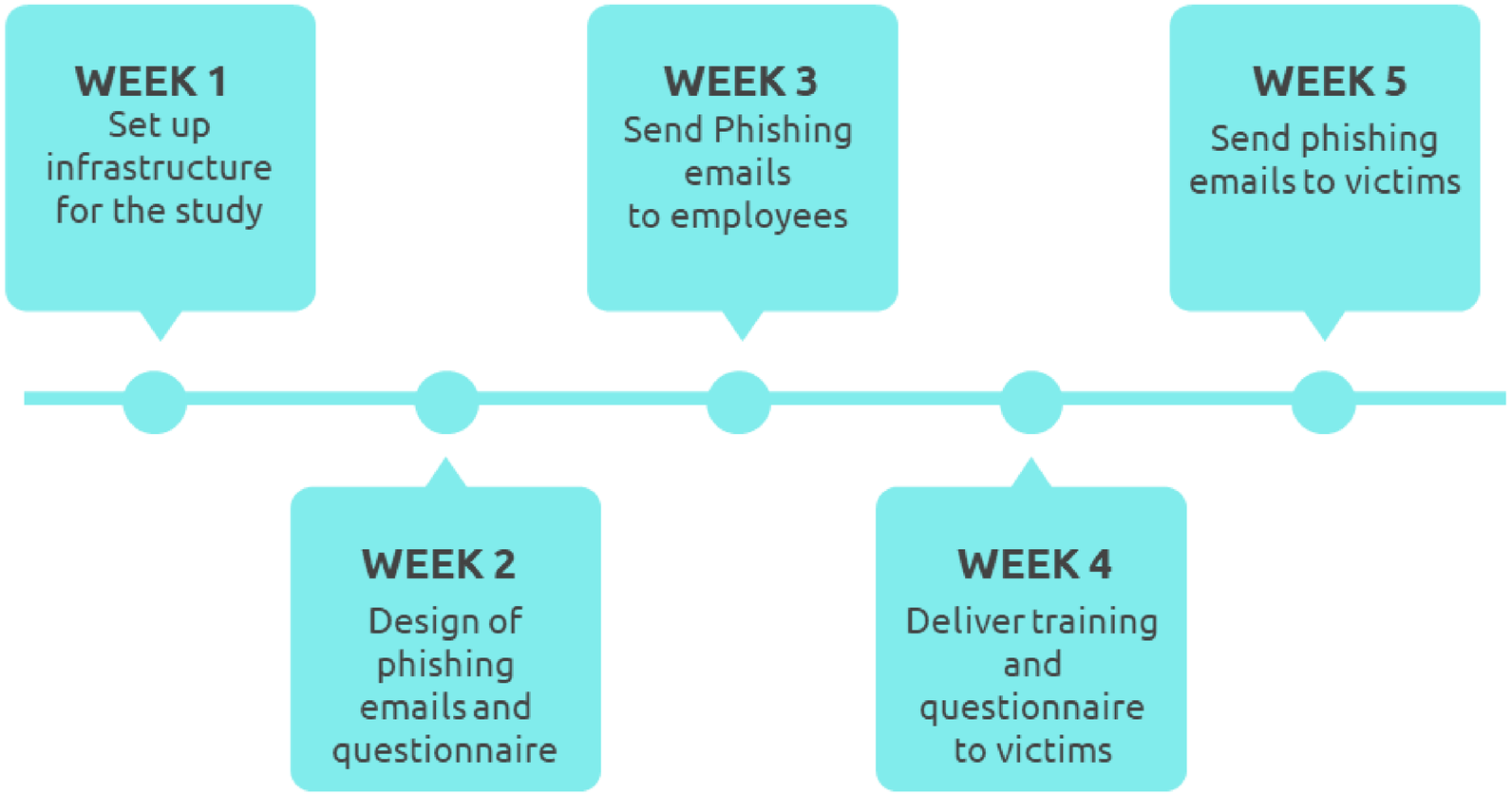
To learn more on how you can start planning your dream vacation, visit our website at < link >.”

Which persuasion technique is more effective?

A Study on Employee's Susceptibility to Phishing

Do **authority** and **urgency** principles increase employee's susceptibility to phishing?

Study Execution



Participants and Experimental Conditions

CONTROL

Received Phishing Emails Not Exploting Persuasion Techniques

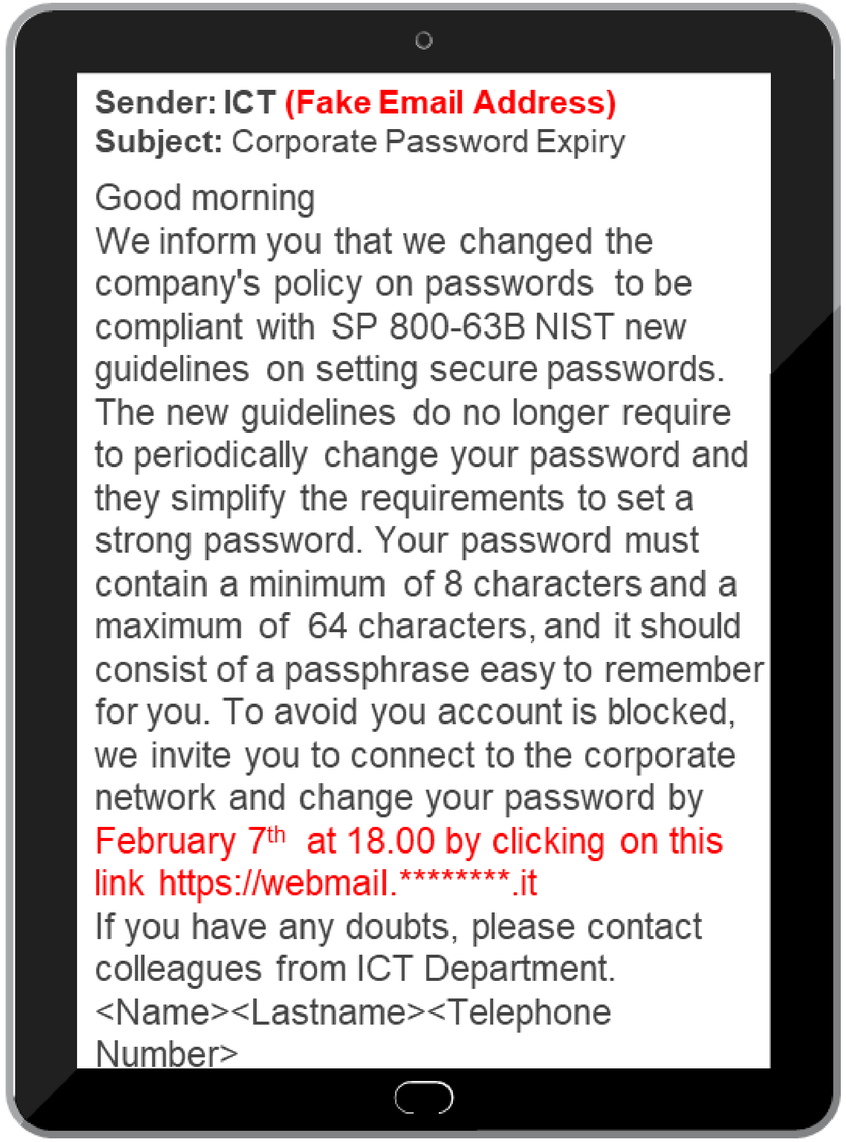
AUTHORITY

Received Phishing Emails coming from someone with a degree of authority within the company

URGENCY

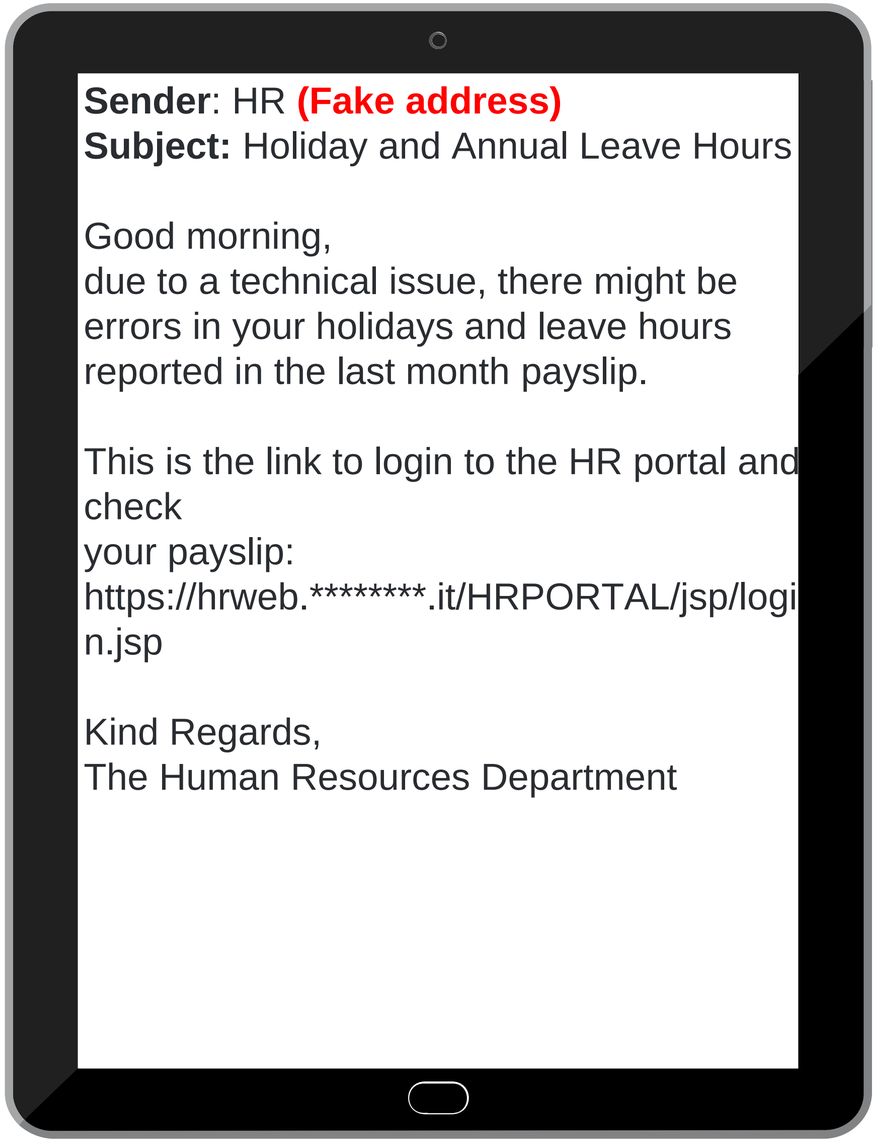
Received Phishing Emails placing employees under time pressure

Email Design



Sender: ICT (Fake Email Address)
Subject: Corporate Password Expiry

Good morning
We inform you that we changed the company's policy on passwords to be compliant with SP 800-63B NIST new guidelines on setting secure passwords. The new guidelines do no longer require to periodically change your password and they simplify the requirements to set a strong password. Your password must contain a minimum of 8 characters and a maximum of 64 characters, and it should consist of a passphrase easy to remember for you. To avoid you account is blocked, we invite you to connect to the corporate network and change your password by February 7th at 18.00 by clicking on this link https://webmail.********.it
If you have any doubts, please contact colleagues from ICT Department.
<Name><Lastname><Telephone Number>



Sender: HR **(Fake address)**
Subject: Holiday and Annual Leave Hours

Good morning,
due to a technical issue, there might be errors in your holidays and leave hours reported in the last month payslip.

This is the link to login to the HR portal and check
your payslip:
https://hrweb.********.it/HRPORTAL/jsp/login.jsp

Kind Regards,
The Human Resources Department

Employees' Susceptibility

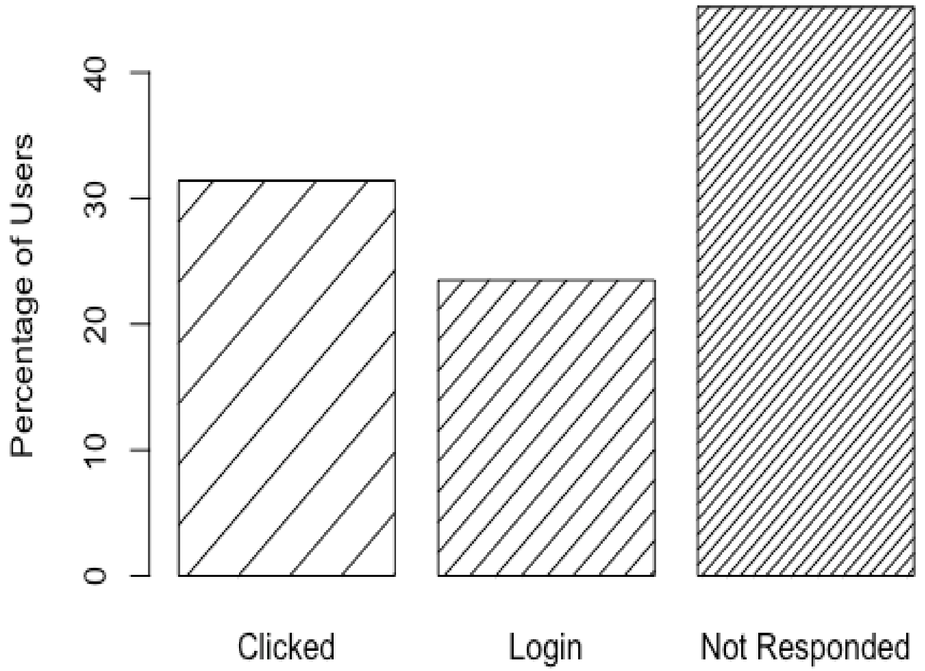
Click Rate

31,4 % of employees clicked the link in the phishing email

Login rate

23.5% of employees provided credentials to the phishing web site

69.2 % of employees who clicked on the link in the phishing then disclose their credentials to the phishing web site



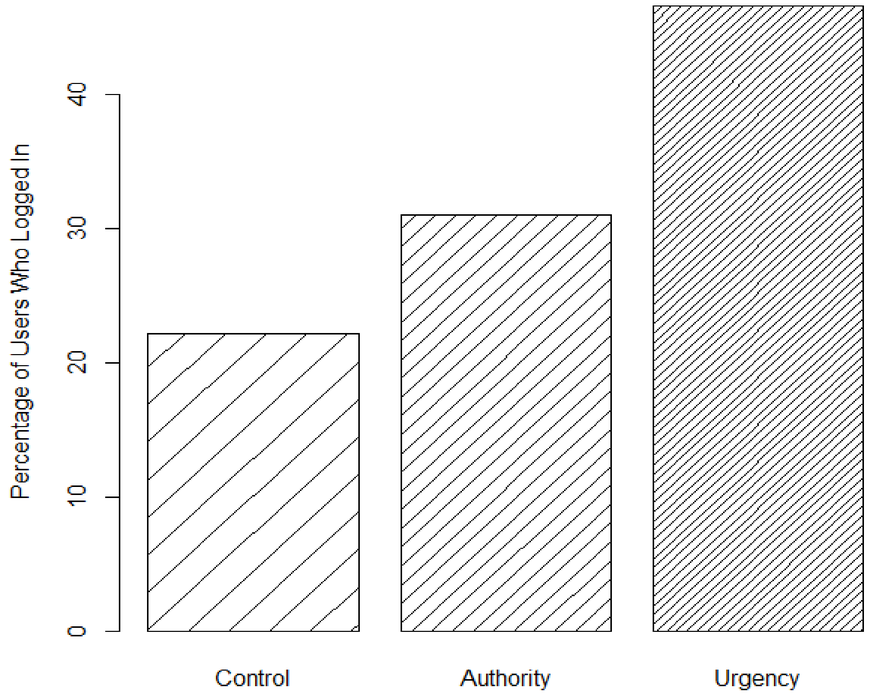
Susceptibility vs Persuasion Principles

Urgency increases employee's susceptibility

33.8% employees were more susceptible to urgency principle

21.5% employees were susceptible to authority principle

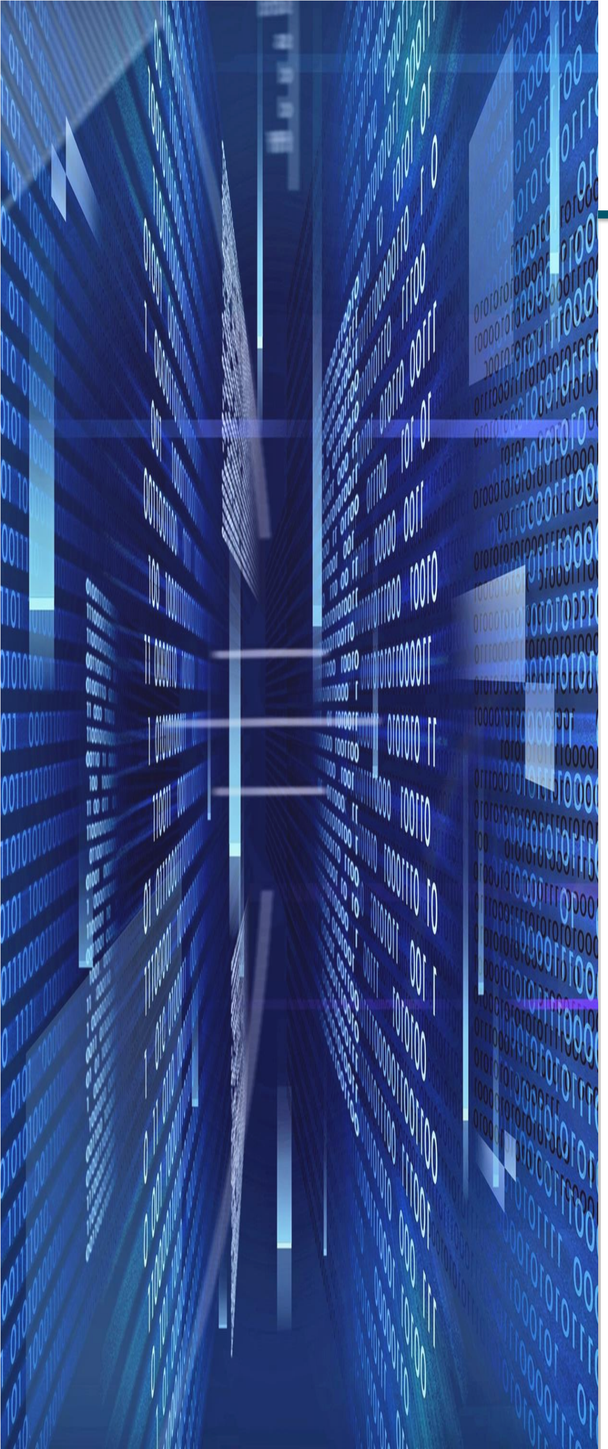
15.6% employees were susceptible to emails not exploiting any persuasion principle



How do employees identify a phishing email?

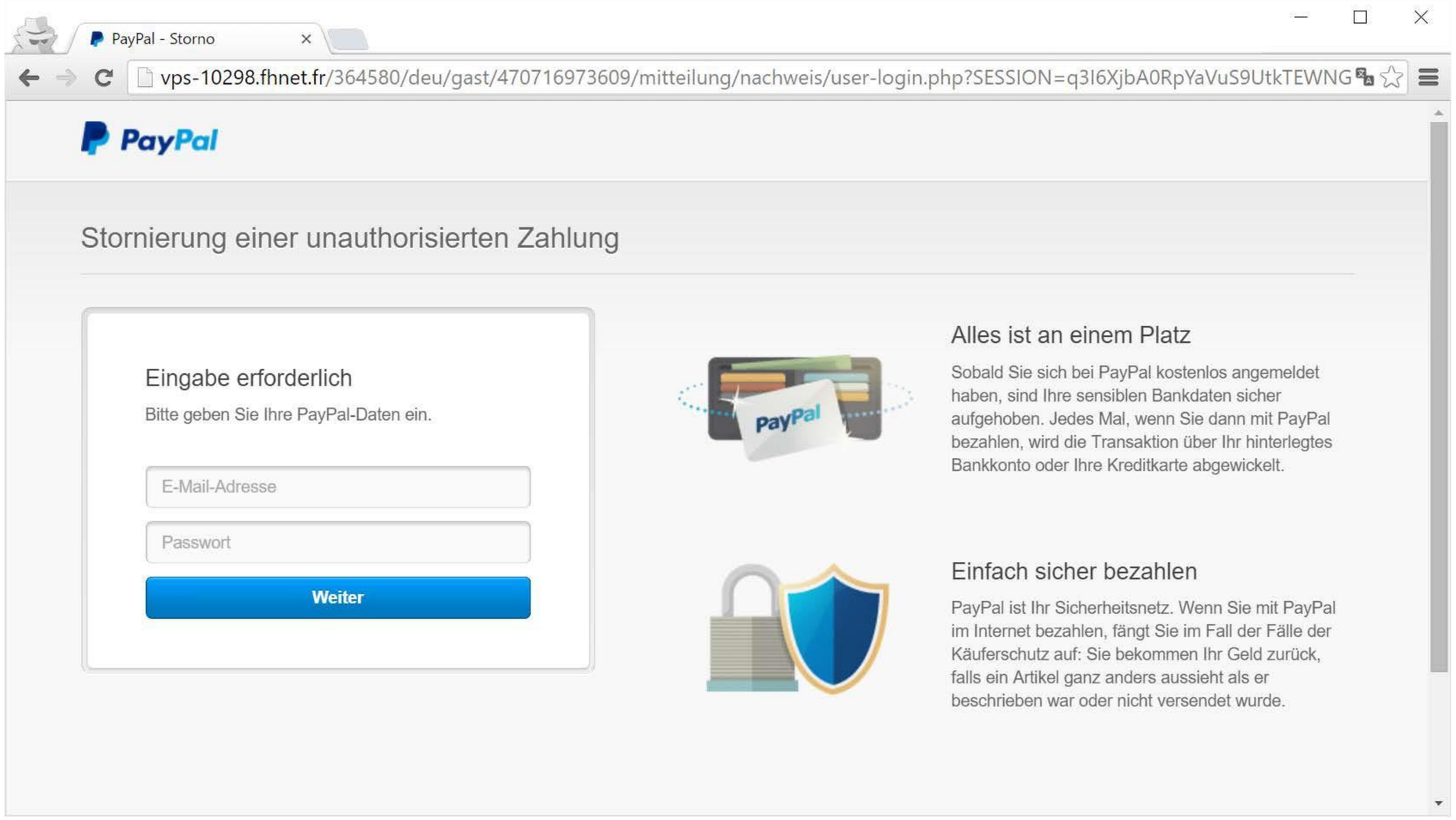
	VICTIMS (%)
EMAIL FORMAT AND CONTENT	66.6
EMAIL SENDER	62.5
EMAIL SIGNATURE	29.16
LINK	20.83

	NON VICTIMS (%)
EMAIL SENDER	32.65
WORK CONTEXT	30.61
EMAIL FORMAT AND CONTENT	18.36
LINK	8.16

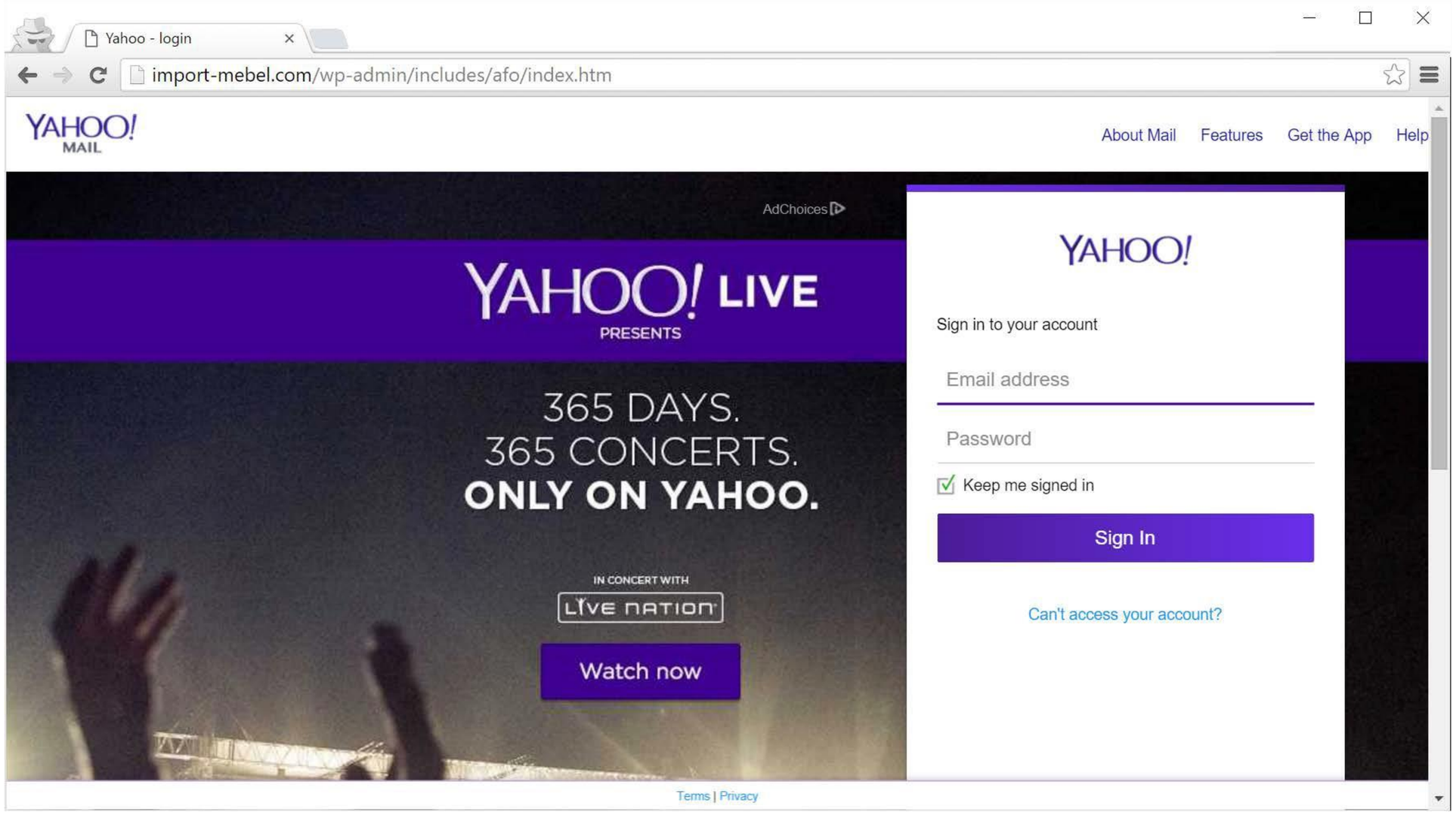


Phishing Websites

Irregular domain names



Missing HTTPS



Is it a phishing a web site?

Is it a phishing web site?

Your account
for everything Apple.

A single Apple ID and password gives you access to all Apple services.

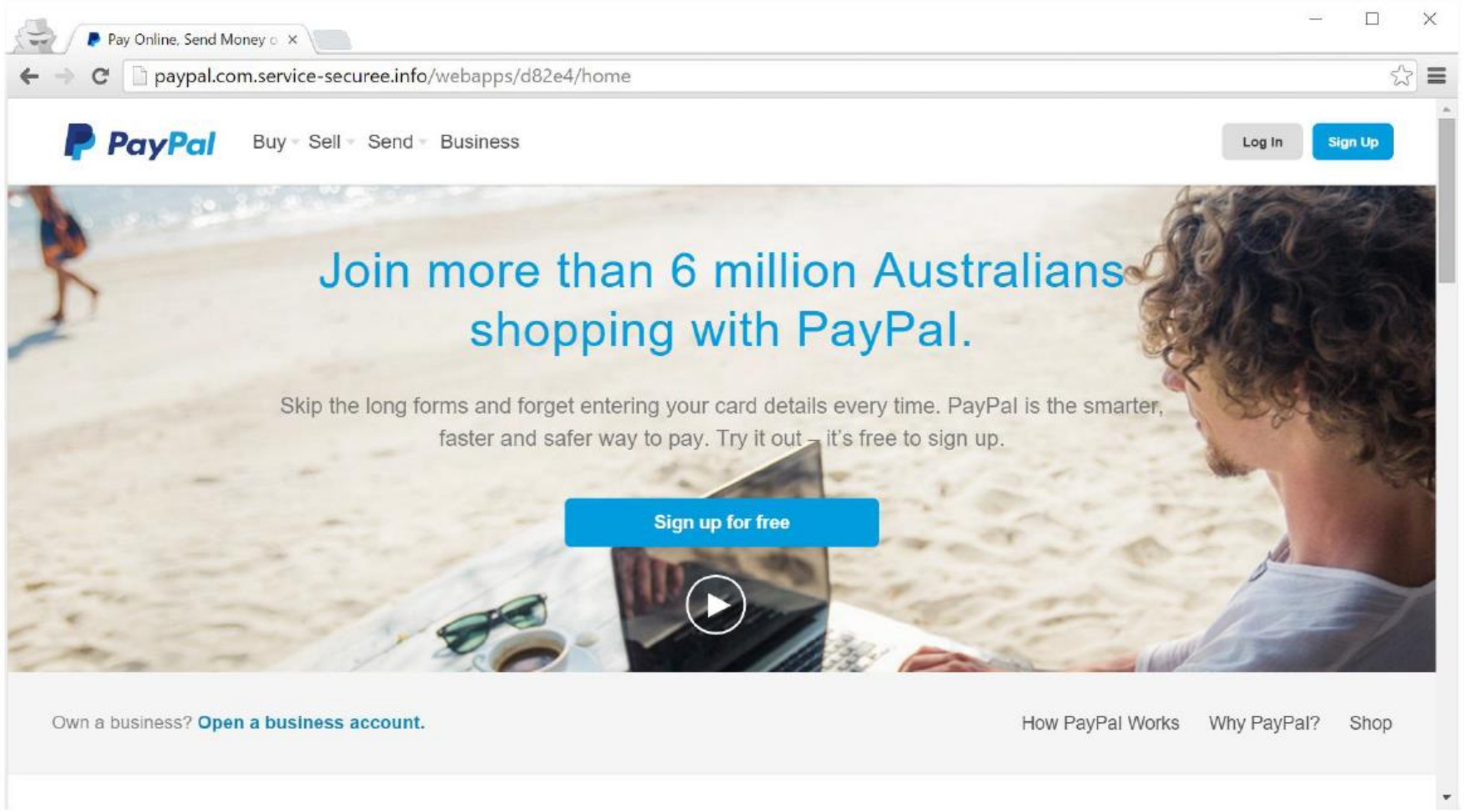
Learn more about Apple ID ›

Your account
for everything Apple.

A single Apple ID and password gives you access to all Apple services.

Learn more about Apple ID ›

(Sub) domain name



Emails with Legitimate Urls

Cloud providers are a top target for phishing attacks

8, 2022

curity, News,
nology

read

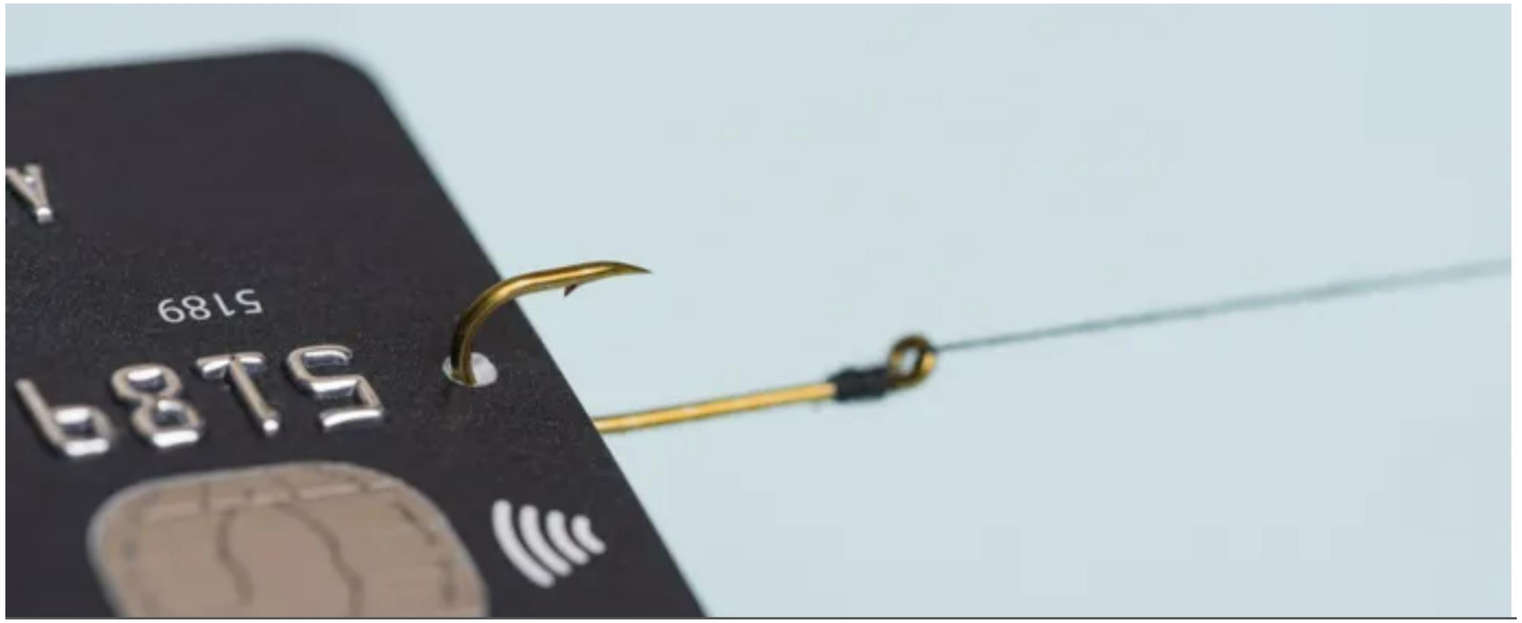
Hijacking Legitimate Web sites

New Phishing Kit Hijacks WordPress Sites for PayPal Scam

Attackers use scam security checks to steal victims' government documents, photos, banking information, and email passwords, researchers warn.

Dark Reading Staff
Dark Reading

July 14, 2022

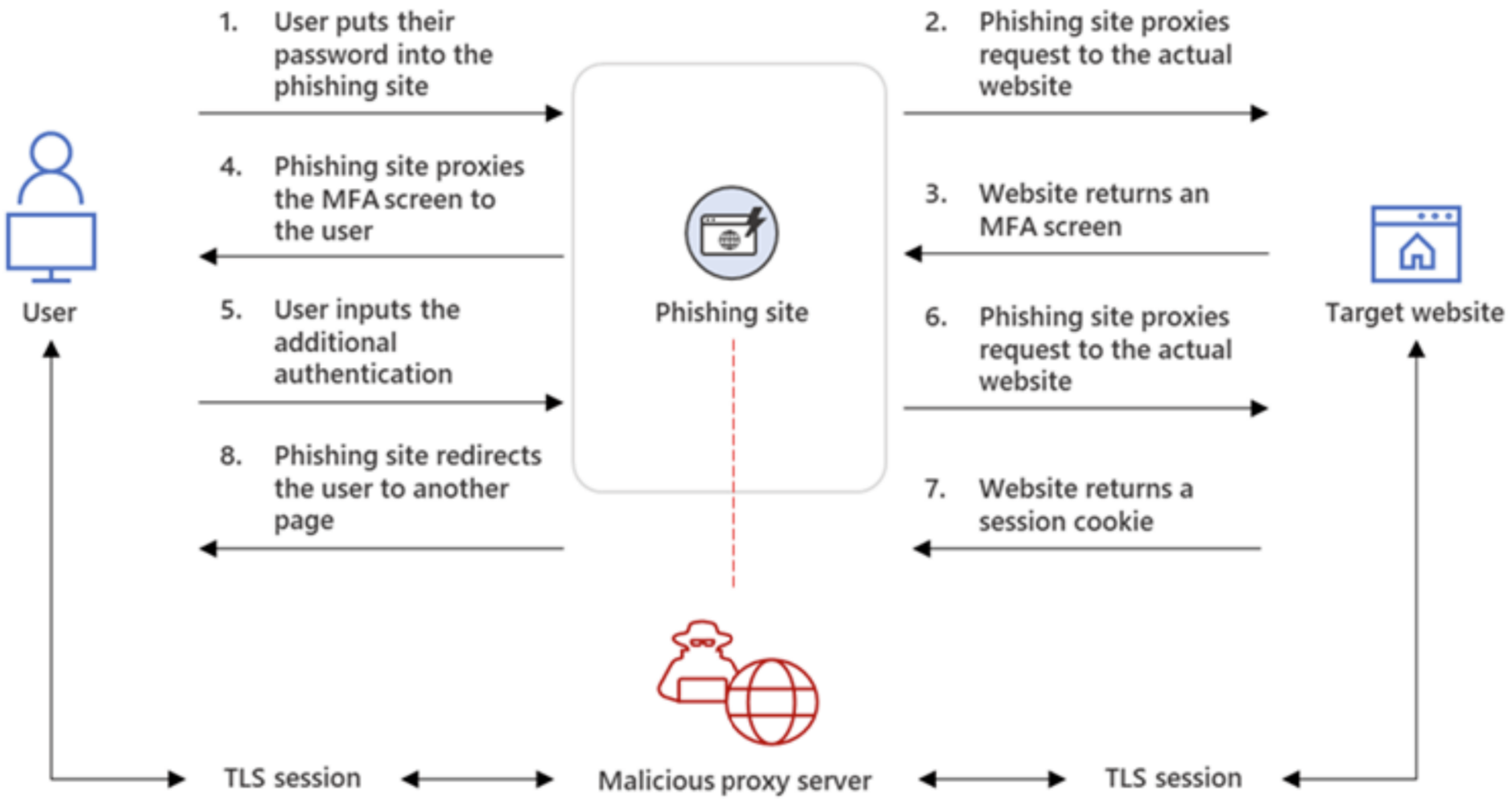


Deepfake Phishing

Deepfakes: Get ready for phishing 2.0

With deepfakes, phishing is evolving once again and being called the most dangerous form of cybercrime.

Phishing as a Service - EvilProxy



Identifying Attacks with PhishTank

PhishTank® Out of the Net, into the Tank.

username
Register | Forgot

Home | Add A Phish | Verify A Phish | Phish Search | Stats | FAQ | Developers | Mailing Lists | My Account

Join the fight against phishing

Submit suspected phishes. Track the status of your submissions.
Verify other users' submissions. Develop software with our free API.

Found a phishing site? Get started now — see if it's in the Tank:

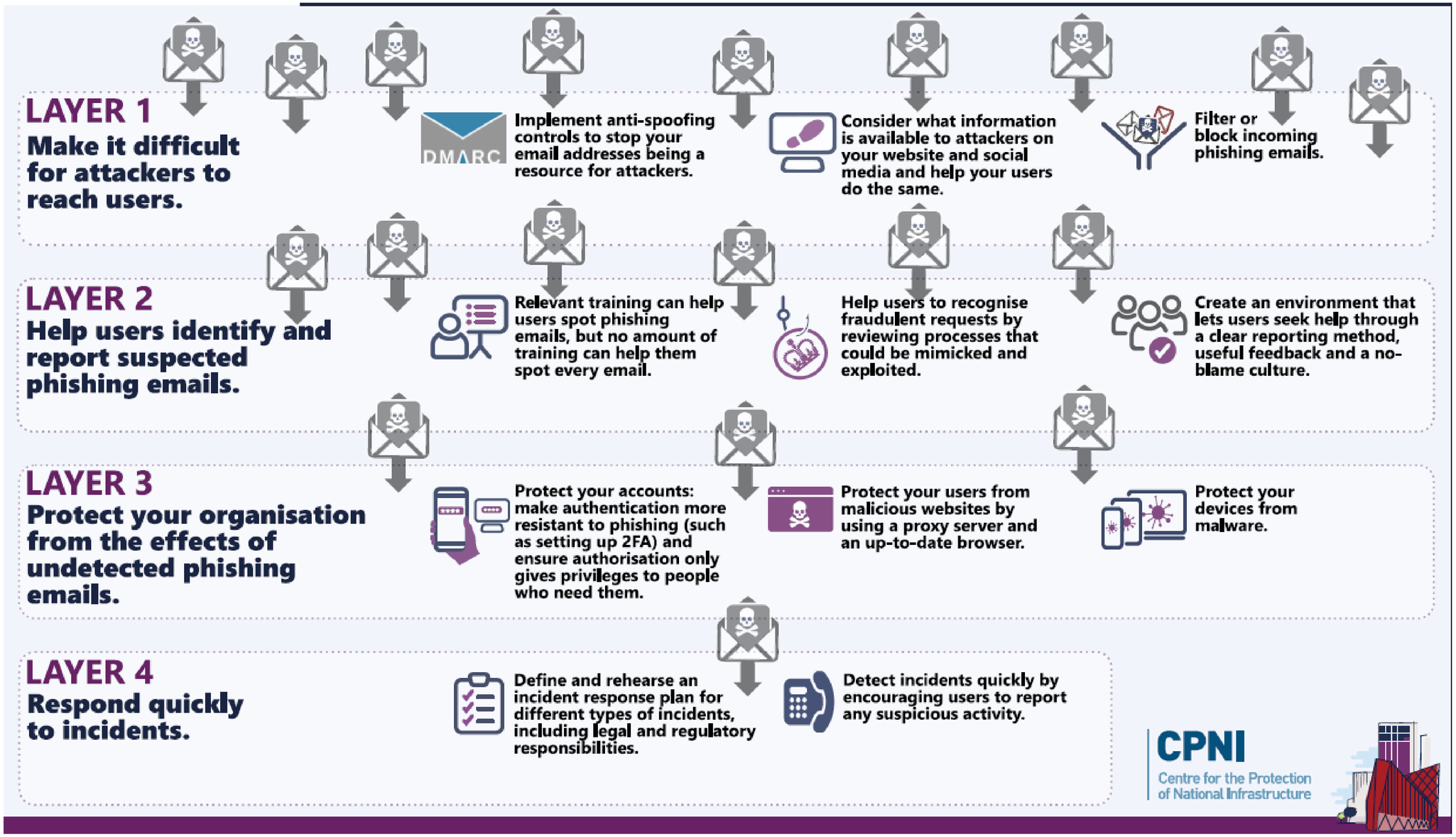
http:// Is it a phish?

Recent Submissions

You can help! Sign in or register (free! fast!) to verify these suspected phishes.

ID	URL	Submitted by
6809267	https://shrt.es/E4GwI	n0x6fb0x6fdy
6809266	https://frikosana.netlify.app/	n0x6fb0x6fdy
6809264	https://pubgxvent.com/	phishb8
6809263	https://pubgmworldevent.com/	phishb8
6809262	https://melcouv.weebly.com/	SWITCHCERT
6809261	https://pfrqguizzwsoittv-dot-glexcel1.ue.r.appspot...	SWITCHCERT
6809260	https://zimwel.weebly.com/	Klug
6809259	https://verify-three.ltd	HKG3GB
6809258	https://billing-verified.co.uk	HKG3GB
6809256	https://www.youtube.com/watch?v=oHg5SJYRHA0	Bexby
6809255	http://document-cloud.com/AfPlyyaxjgvq	Bexby
6809254	https://secure.oldschool.com-er.ru/m=forum/forums....	Solveig
6809253	https://palgsovetnyk.ru/wp-includes/css/dist/Popul	phishpopularbank

How an organization can stop phishing attacks?



Resources

- **The social engineering framework.** https://www.social-engineer.org/framework
- Persuasion principles. https://www.social-engineer.org/framework/influencing-others/
- Marco DeBona, Federica Paci. **A real world study on employees' susceptibility to phishing attacks.** ARES '20: Proceedings of the 15th International Conference on Availability, Reliability and Security https://dl.acm.org/doi/abs/10.1145/3407023.3409179
- Phishing attacks: defending your organization https://www.ncsc.gov.uk/guidance/phishing#downloads
- https://beefproject.com/