



Social Engineering Attacks

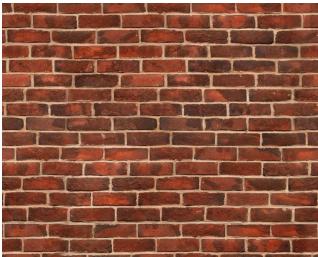
Mariano Ceccato

mariano.ceccato@univr.it



What is social engineering

- Psychological manipulation of people into performing actions or divulging personal information



Firewall



Access control



Anti virus



End users



President Macron's Identity Theft

WORLD NEWS

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."



By Associated Press | Associated Press, Paris

UPDATED ON MAR 14, 2018 05:01 PM IST



French President Emmanuel Macron addresses the media at the Elysee Palace in Paris, France, March 8, 2018.(Reuters)

<https://www.hindustantimes.com/world-news/two-frenchmen-on-trial-for-stealing-president-macron-s-online-identity/story-tpEIBRZRGi1PYToHTGIHxO.html>



Facebook Lottery Scam



- Notification of 500k\$ winning
- FBI is involved
- A friend in your network contacts you with a positive experience with this
- Some money are needed to unlock the winning

<https://www.scamwatch.gov.au/get-help/real-life-stories/unexpected-prize-lottery-scam-davins-fictional-facebook-lottery-win>



Types of Social Engineering Attacks

Computer Based

- Phishing
- Spear phishing
- Whaling
- Viral hoax

Human Based

- Vishing
- Impersonation
- SMiShing
- Tailgating



Phishing



Agenzia delle Entrate - Amministrazione fiscale

Con la presente ti informiamo che nel tentativo di rimborsare l'account l'operazione non è andata a buon fine.

Accedi al tuo portale di rimborso delle tasse per elaborare manualmente il rimborso. Durante il processo, è possibile aggiornare le informazioni dell'account fornite. [AGGIORNARE](#).

Data di pagamento: 30 Giugno 2018

Numero della fattura: ADE / P881P29 / IT2001

Importo: €1,482.05 EUR

NOTA BENE: Questa E-Mail è un documento di fatturazione ufficiale per il rimborso.

<https://www.agenziaentrate.gov.it/portale/web/guest/-/cs-30072018-mail-truffa>



Viral hoax

- Coronavirus: pandemic virus conspiracy video spreads across social media

facebook [Sign Up](#)

Email or phone Password [Log In](#)

[Forgotten account?](#)



Aproko freedom commenters
27 May at 03:24 ·

THE GAME IS OVER, ITALIAN DOCTORS FINALLY UNCOVERS W.H.O AGENDA. SAYS CORONAVIRUS CURE WAS HIDDEN FROM THE WORLD...

Italian doctors, disobeyed the world health law WHO, not to do autopsies on the dead of the Coronavirus and they found that it is NOT a VIRUS but a BACTERIA that causes death. This causes blood clots to form and causes the death of the patient.

- ◆ Italy defeats the so-called Covid-19, which is nothing other than "Disseminated intravascular coagulation" (Thrombosis).
- ◆ And the way to combat it, that is, its cure, is with the "antibiotics, anti-inflammatories and anticoagulants". ASPIRIN, indicating that this disease had been poorly treated. This sensational news for the world has been produced by Italian doctors by performing autopsies on corpses produced by the Covid-19.
- ◆ Something else, according to Italian pathologists. "The ventilators and the intensive care unit were never needed."
- ◆ Therefore in Italy the change of protocols began, ITALY THE SO-CALLED global pandemic is REVEALED AND RAISED BY THE WHO, this cure the Chinese already knew and did not report FOR DOING BUSINESS.

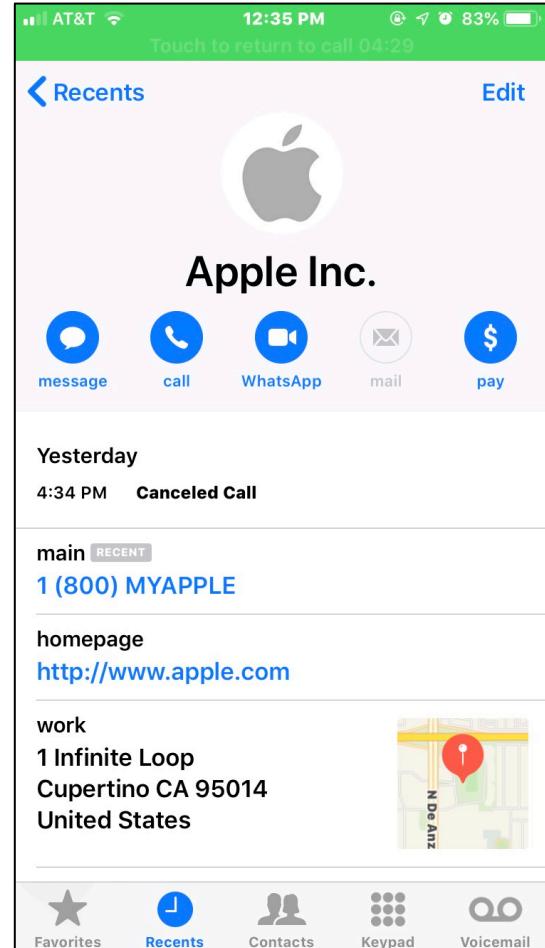
Source: ITALY Ministry of Health.

SHARE THAT THE WORLD KNOWS THAT WE HAVE BEEN DECEIVED AND MURDERED BY OUR OLDER PERSONS !!!



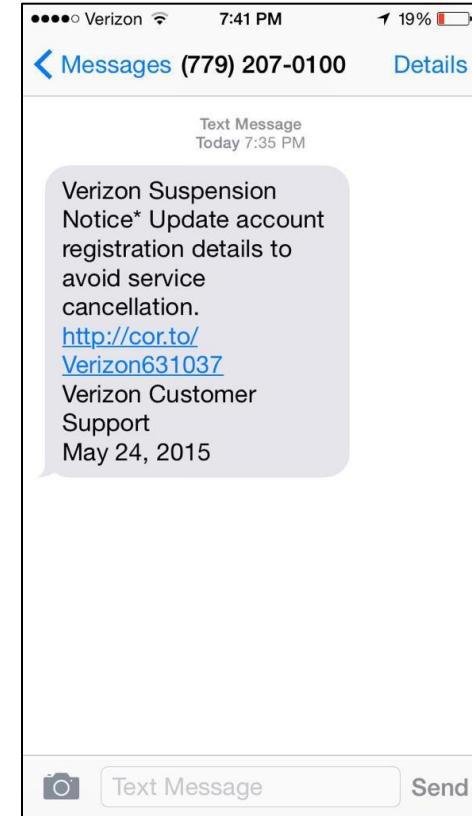
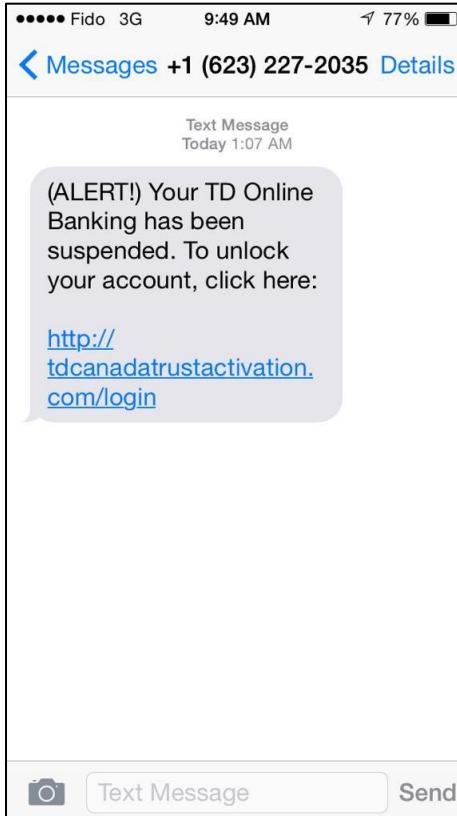
Vishing – voice phising

- Receiving phone calls that look legitimate
- Asking for personal information to solve security issues





SMiShing – SMS Phishing





Tailgating, Piggybacking





Phishing

- Attempt to acquire sensitive information (often for malicious reasons) by masquerading as a trustworthy entity in an electronic communication
 - Information: usernames, passwords, and credit card details (and sometimes, indirectly, money)



Gmail blocked more than 100M phishing emails

Solidarity Response Fund. Help WHO fight COVID-19 ➔ Spam ×

2:16 PM (2 hours ago) ⚡ ⓘ

This message seems dangerous

Similar messages were used to steal people's personal information. Avoid clicking links, downloading attachments, or replying with personal information.

Looks safe

The world has never faced a crisis like COVID-19. The pandemic is impacting communities everywhere. **It's never been more urgent to support the global response.** The humanity, solidarity and generosity of people and organizations everywhere is also unprecedented. But we can't stop now.

The World Health Organization (WHO) is leading and coordinating the global effort with a range of partners, supporting countries to prevent, detect, and respond to the pandemic. **Donations support WHO's work, including with partners, to track and understand the spread of the virus; to ensure patients get the care they need and frontline workers get essential supplies and information; and to accelerate research and development of a vaccine and treatments for all who need them.**

See below for more ways to give, Via BTC (Bitcoin). Every donation helps support life-saving work for the world.

BTC Address: *****



Massive Phishing Attack against Gmail users

Joe Bernstein has shared a document on Google Docs with you



Inbox x



joe.bernstein@buzzfeed.com

✉ to hhhhhhhhhhhhhhh., bcc: zeynep ▾

Joe Bernstein has invited you to view the following document:

[Open in Docs](#)



Target data breach

Target to Pay \$18.5 Million to 47 States in Security Breach Settlement



Target's headquarters in Minneapolis. A settlement by the company ended an investigation into how the data of millions of customers was compromised in 2013. Glen Stubbe/Star Tribune, via Associated Press

By Rachel Abrams

May 23, 2017

Target will pay \$18.5 million to 47 states and the District of Columbia as part of a settlement with state attorneys general over a huge security breach that compromised the data of millions of customers.

The settlement ends a yearslong investigation into how hackers obtained names, credit card numbers and other information about tens of millions of people in 2013.

New York will receive \$635,000, while California will receive \$1.4 million, the largest amount of any state, according to the Eric T. Schneiderman, New York's attorney general. Dollar figures were determined "largely" based on each state's population size, his office said.

Wyoming, Wisconsin and Alabama were not included in Tuesday's announcement. Representatives for the attorneys general in those states did not have an immediate comment or could not be reached.

<https://www.nytimes.com/2017/05/23/business/target-security-breach-settlement.html>



Phisching emails



PayPal Phishing Scam

+ New Delete Archive Not junk | Block Move to Categories Empty

Notice : Your Account PayPal Has Been Limited !

PayPal Inc. (services@apple.com) Add to contacts ! 06/05/2015

To:

From: PayPal Inc. (services@apple.com) Microsoft SmartScreen classified this message as junk.
Sent: 06 May 2015 22:29:05

To: |

Microsoft SmartScreen marked this message as junk and we'll delete it after ten days.
Wait, it's safe!

PayPal

Your Account PayPal Has Been Limited !

Dear Customer,

To get back into your PayPal account, you'll need to confirm your identity.

It's easy:

1. Click on the link below or copy and paste the link into your browser.
2. Confirm that you're the owner of the account, and then follow the instructions.

<http://www.confirm-identity.me.ma/>

Thank You.

21/04/21



Hyperlink target mismatch

Sun 20/12/2015 02:13

Outlook1.Microsoft.Hotmail.message.1.lbjlvkhjfc-40347323lb@_lbjlv403cutomSignIn.loofking.pitchup.com
[ACCOUNT-ALERT:40347323106006042083-LBJ]

To: [REDACTED]@hotmail.com
Cc: 4034732310@r184.admarketing.guess.ca

If there are problems with how this message is displayed, click here to view it in a web browser.

Outlook December 19 2015

Dear Account E-mail Holder([REDACTED][hotmail.com](mailto:[REDACTED]hotmail.com)),

We're having a problem verifying your email account information.

You might not be able to see all your email messages due to several security concerns.

We will start working on fixing the problem as soon you verify your account details.

Please check your login details by following our secure link:

<http://greenplantagro.com/otlk/index.php>
Click or tap to follow link.

<https://outlook.com/?Joig-CA&refd=verify&user=troyhunt@hotmail.com>

If your email information is not updated within 24 hours your email account might expire.



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



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.



John Podesta spearphishing attack



myaccount.google.com-securitysettingpage.tk

Someone has your password

<http://myaccount.google.com-securitysettingpage.tk/security/signinoptions/password?e=am9obi5wb2Rlc3RhQGdtYWlsLmNvbQ%3D%3D&fn=Sm9obiBQb2Rlc3Rh&n=Sm9obg%3D%3D&img=Ly9saDQuZ29vZ2xldXNlcmNvbnRlbnQuY29tLy1RZVlPbHJkVGp2WS9BQUFBQUFBSS9BQUFBQUFBQUFCTS9CQIdVOVQ0bUZUWS9waG90by5qcGc%3D&id=1sutlodlw>

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.

bit.ly/1PibSU0

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.



John Podesta spearphishing attack

The screenshot shows a web browser window with the URL <http://myaccount.google.com-securitysettingpage.tk/security/sign> in the address bar. The page itself is a Google sign-in screen, featuring the Google logo and the tagline "One account. All of Google." Below this, there is a "Sign in to continue to Gmail" link. A large, semi-transparent overlay box is centered over the sign-in form. Inside this box, there is a placeholder profile picture of John Podesta, his name "John Podesta", and his email address "john.podesta@gmail.com". Below this, there is a password input field labeled "Password" and a blue "Sign in" button. At the bottom of the overlay, there is a link "Need help?". At the very bottom of the page, outside the overlay, there is a link "Sign in with a different account" and a footer note "One Google Account for everything Google".



Spearphishing and Extortion

Question - Message (HTML)

File Message Tell me what you want to do

 Sun 27/09/2015 01:52
[redacted]

Question

To troyhunt@hotmail.com

Unfortunately your data, including complete credit card details, was leaked in the recent hacking of Ashley Madison. Below is the glimpse of the data we have about you:

Name: [redacted]
Address: [redacted], US
Credit Card Type Used: MC
Credit card number: [redacted]
Last Payment: 168.99 on 2013-10-[redacted]
Your computer ip address: [redacted]

Plus we have access to your complete profile data including your pics, secret fantasies, conversations, etc.

We have access to your Facebook page as well. If you would like to prevent me from sharing this dirt info with all of your friends, family members, spouse, then you need to send exactly 5 bitcoins (BTC) to the following BTC address:

Bitcoin Address:
19tdydCA6nRX73HG5MsozGtDdSLN8L^Esus

We are providing a chance to solve this case. You make a payment to the above mentioned btc address. The time ends in the next 24 hours. We will not publish your data and we will not inform your contacts.

You can get bitcoins at an exchange like Expresscoin.com, Localbitcoins.com, Clevercoin.com, Coincorner.com, Coincafe.com, Coinbase.com, Circle.com or a Bitcoin ATM machine Coinatmradar.com.



Whaling

- A form of spearphishing that targets high-ranking victims within a company
 - E.g. CFO and CEO

WHITE PAPERS



Akamai Executive Briefing: 2019 Gartner Critical Capabilities for...



The Forrester Wave™: Web Application Firewalls, Q1 2020



Conquering the Cloud: Data Security and Compliance with a CASB



Influence Tactics



Exploiting Authority

Screenshot of an email from the Agenzia delle Entrate (Italian Tax Agency) to help <famiglia@gretaboesel.com>. The email is dated 09:20 and includes the recipient's name, IL DIRETTORE DELL'AGENZIA DELLE ENTRATE 38596916.

The email body contains the Agenzia delle Entrate logo and the Italian Republic emblem (Stato Italiano).

Text in the email:

- 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.

Attachment icon: ZIP file named 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

Van: Facebook [mailto:notification+zrdohyri=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!

[malicious 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 malicious link



Phishing Websites

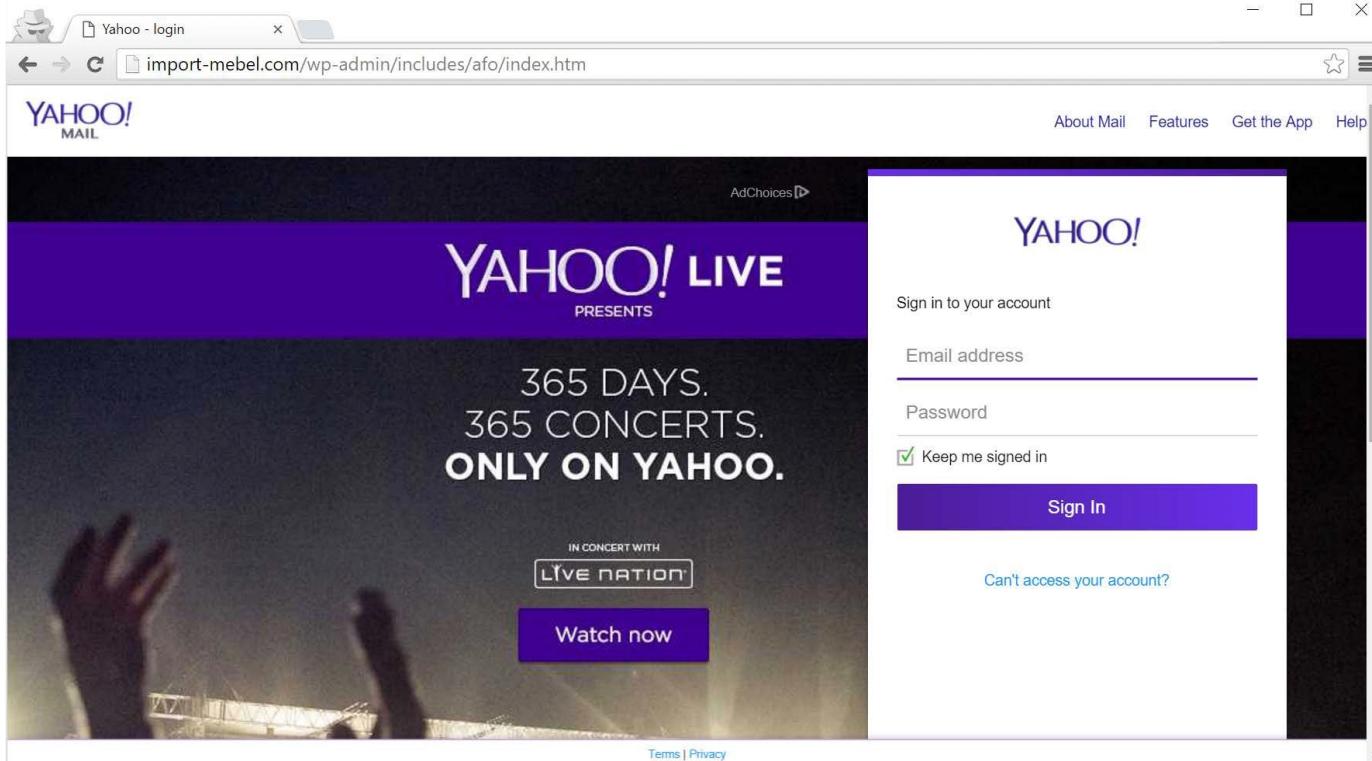


Irregular domain names

The screenshot shows a web browser window with the title "PayPal - Storno". The URL in the address bar is "vps-10298.fhnet.fr/364580/deu/gast/470716973609/mitteilung/nachweis/user-login.php?SESSION=q3I6XjbA0RpYaVuS9UtkTEWNG". The main content is a "Stornierung einer unauthorisierten Zahlung" (Cancellation of an unauthorized payment) page. On the left, there is a form with fields for "E-Mail-Adresse" and "Passwort" (Email Address and Password), and a blue "Weiter" (Continue) button. To the right of the form, there is a graphic of a credit card and a PayPal envelope. Below this graphic, the text "Alles ist an einem Platz" (Everything in one place) and "Sobald Sie sich bei PayPal kostenlos angemeldet haben, sind Ihre sensiblen Bankdaten sicher aufgehoben. Jedes Mal, wenn Sie dann mit PayPal bezahlen, wird die Transaktion über Ihr hinterlegtes Bankkonto oder Ihre Kreditkarte abgewickelt." (As soon as you log in to PayPal for free, your sensitive bank details are safely stored. Every time you pay with PayPal, the transaction is processed through your stored bank account or credit card.) To the right of the card graphic, there is a graphic of a padlock and shield, with the text "Einfach sicher bezahlen" (Simply safe payment) and "PayPal ist Ihr Sicherheitsnetz. Wenn Sie mit PayPal im Internet bezahlen, fängt Sie im Fall der Fälle der Käuferschutz auf: Sie bekommen Ihr Geld zurück, falls ein Artikel ganz anders aussieht als er beschrieben war oder nicht versendet wurde." (PayPal is your safety net. When you pay online with PayPal, the buyer protection kicks in: you get your money back if an item looks nothing like it was described or isn't delivered.)



Missing HTTPS





(Sub) domain name

A screenshot of a web browser window displaying the PayPal login page. The URL in the address bar is paypal.com.service-securee.info/webapps/d82e4/home. The page features the PayPal logo and navigation links for Buy, Sell, Send, and Business. On the right, there are 'Log In' and 'Sign Up' buttons. The main content area has a large image of a man with curly hair sitting at a beach, looking at a laptop. Text on the page reads: 'Join more than 6 million Australians shopping with PayPal.' Below this, a subtext says: 'Skip the long forms and forget entering your card details every time. PayPal is the smarter, faster and safer way to pay. Try it out – it's free to sign up.' A prominent blue button with the text 'Sign up for free' and a play icon is centered over the image. At the bottom, there are links for 'Open a business account.', 'How PayPal Works', 'Why PayPal?', and 'Shop'.



Website Hijacking

The screenshot shows a web browser window with the URL www.supreme9events.com/pyramid/javascripts/online/verification/database-update/wellsfargo.com/. The page is designed to look like the official Wells Fargo website, featuring the Wells Fargo logo and navigation links for Personal, Small Business, Commercial, Financial Education, and About Wells Fargo. The main content area displays a 'View Your Accounts' form with fields for Username and Password, and links for Account Summary, Go, and Username / Password Help. Below this is a promotional banner for checking and savings accounts, featuring a smiling couple and a child, with the text 'We know your time is valuable' and 'Start Now'. At the bottom, there are links for Fraud Information Center, Banking Made Easy, Going to College, Home Lending, Borrowing and Credit, and Managing your money for college.



Identifying Attacks with PhishTank

PhishTank® Out of the Net, into the Tank.

username
[Register](#) | [Forgot Password?](#)

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:
 [Is it a phish?](#)

Recent Submissions

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

ID	URL	Submitted by
6965114	https://www.homeaddresspost.website/...	GovCERTCH
6965113	https://igseo.org/diepost/manage/	GovCERTCH
6965110	https://www.airbnb.de/external_link?c=.pi80.pkb2iu...	cleanmx ↗
6965109	https://sites.google.com/view/bt-business-voice/bt...	verifrom
6965108	<a href="http://rakutnn.co.jp.gtqkz4e2.cc/?account_login?=<...">http://rakutnn.co.jp.gtqkz4e2.cc/?account_login?=<...	hideaki
6965107	<a href="http://rakutnn.co.jp.1snuahg4.cc/?account_login?=<...">http://rakutnn.co.jp.1snuahg4.cc/?account_login?=<...	hideaki
6965106	https://mailserver28.godaddysites.com/	verifrom
6965105	https://complete-pay.online	BDWZCKGP
6965104	https://australiacartransport.com.au/	GMc70
6965103	http://australiacartransport.com.au	GMc70
6965102	<a href="http://rakutnn.co.jp.2qibw0oq.cc/?account_login?=<...">http://rakutnn.co.jp.2qibw0oq.cc/?account_login?=<...	hideaki
6965101	https://declinicense.com/az/admin/	PhishReporter
6965100	https://bt-hub.weebly.com/	verifrom
6965099	http://ppb-acesso.com/bb/	csintbb
6965098	https://legislaturepassword.com/ING/r4/index.php	BPhv

[See more suspected phishes...](#)

New to PhishTank?

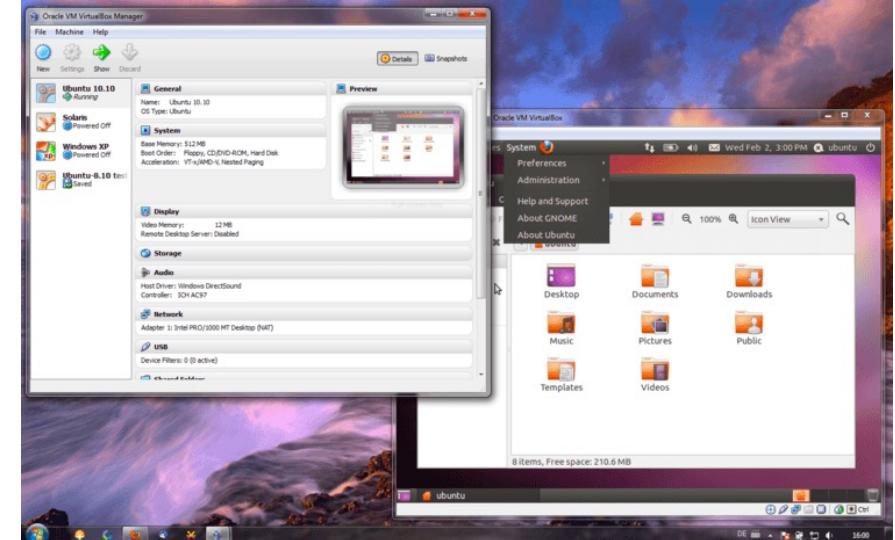
[Subscribe](#) to the PhishTank mailing lists.

Prof Mariano Ceccato, a.a. 2020-2021



Virtual box

- High performance virtualization tool, to run a *guest OS* in your *host OS*
- Support for multiple host OSes
- <https://www.virtualbox.org/>





Kali Linux – offensive security

- Linux distribution maintained and funded by Offensive Security
- Designed for digital forensics and penetration testing
- Many security auditing tools are pre-installed and configured
 - exploiting a victim network or application
 - performing network discovery/scanning
 - scanning a target IP address
 - penetration testing
 - password crack
- <https://www.offensive-security.com/kali-linux-vm-vmware-virtualbox-image-download/>