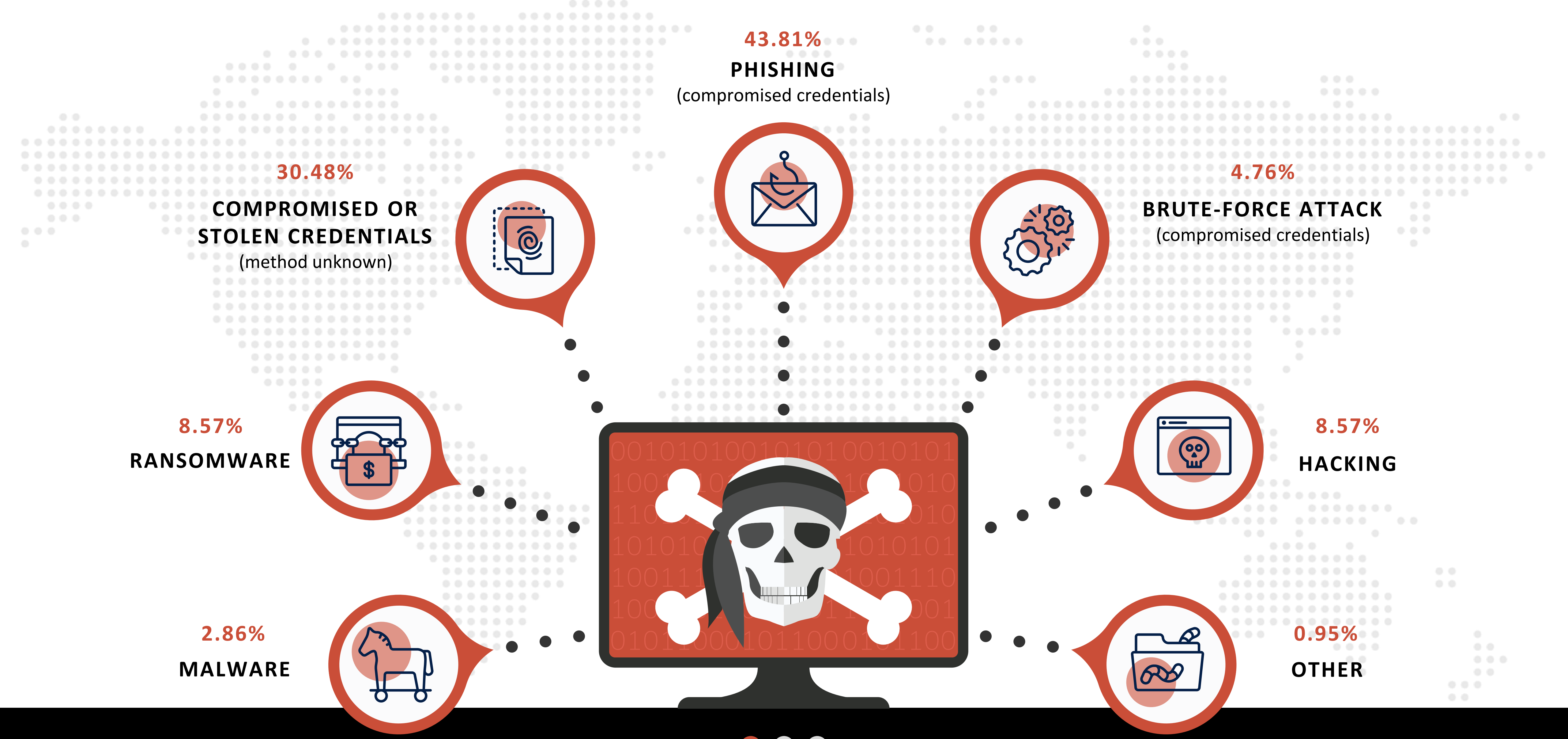
Digital Risk:

Using Dark Web Monitoring to Protect your most important asset

Incident Response

FORENSIC & CYBER

HOW ARE ALL THESE BREACHES HAPPENING?



30.48%

COMPROMISED OR STOLEN CREDENTIALS

(method unknown)

43.81%

PHISHING

(compromised credentials)

4.76%

BRUTE-FORCE ATTACK

(compromised credentials)

8.57%

RANSOMWARE

8.57%

HACKING

2.86%

MALWARE

0.95%

OTHER

THE THREAT TO ALL BUSINESS

9 Ways your employees' work credentials can lead to a breach

HR & PAYROLL

PAYCHEX

ADP

CERIDIAN

EMAIL SERVICES

Office 365

YAHOO!

CRM

salesforce

HubSpot

ZOHO

TRAVEL SERVICES

Expedia

travelocity

ORBITZ

FASTBOOKING

COMMUNICATIONS

verizon

AT&T

Adobe

T · · Mobile ·

E-COMMERCE

STAPLES

ebay

amazon

Office DEPOT

BANKING & FINANCE

intuit quickbooks

Bank of America

freshdesk

COLLABORATION

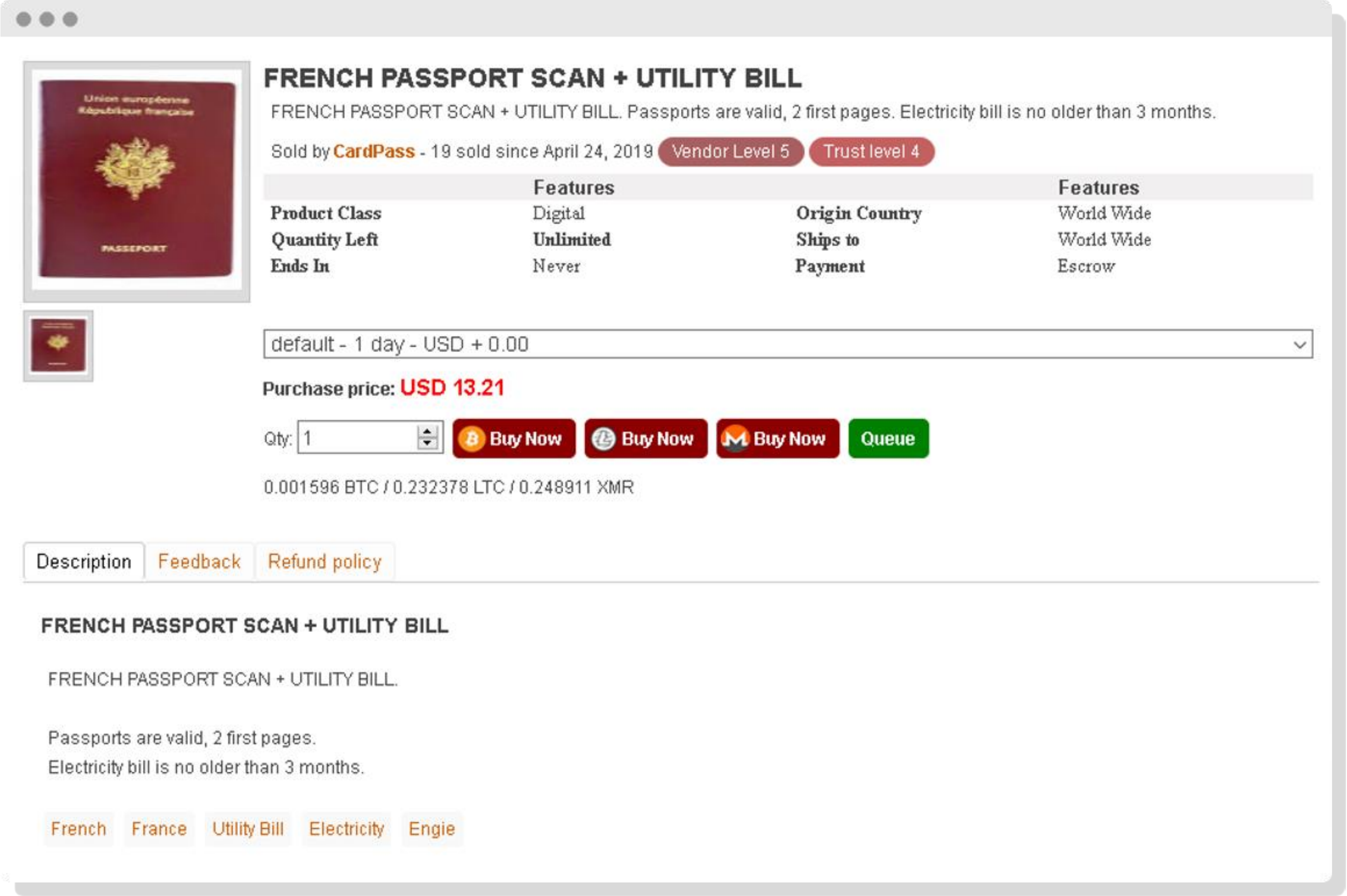
CITRIX

box

Dropbox

SOCIAL MEDIA

THE DARK WEB IS REAL



FRENCH PASSPORT SCAN + UTILITY BILL

FRENCH PASSPORT SCAN + UTILITY BILL. Passports are valid, 2 first pages. Electricity bill is no older than 3 months.

Sold by CardPass - 19 sold since April 24, 2019 Vendor Level 5 Trust level 4

	Features		Features
Product Class	Digital	Origin Country	World Wide
Quantity Left	Unlimited	Ships to	World Wide
Ends In	Never	Payment	Escrow

default - 1 day - USD + 0.00

Purchase price: USD 13.21

Qty: 1

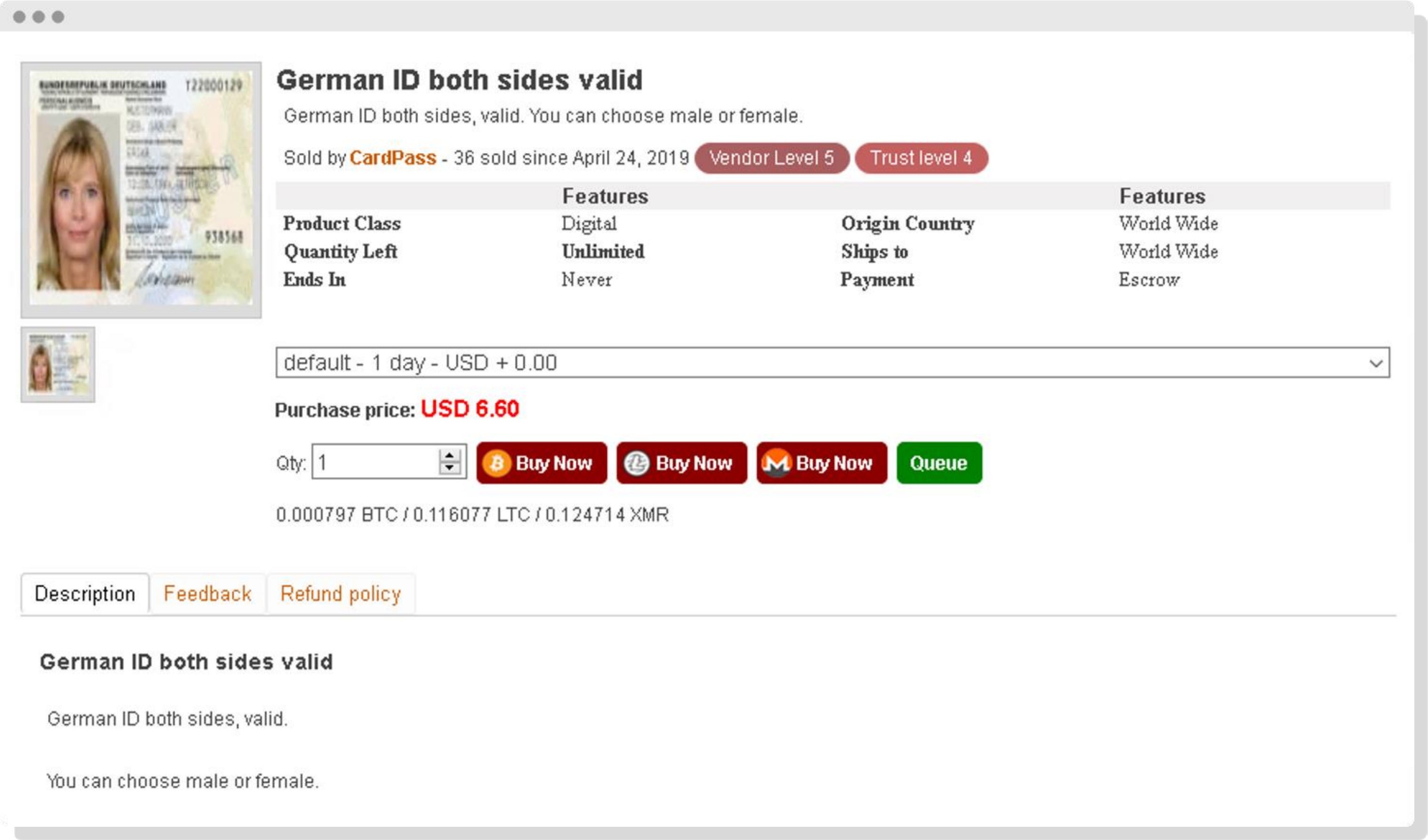
0.001596 BTC / 0.232378 LTC / 0.248911 XMR

FRENCH PASSPORT SCAN + UTILITY BILL

FRENCH PASSPORT SCAN + UTILITY BILL.

Passports are valid, 2 first pages.
Electricity bill is no older than 3 months.

THE DARK WEB IS REAL



German ID both sides valid

German ID both sides, valid. You can choose male or female.

Sold by CardPass - 36 sold since April 24, 2019 Vendor Level 5 Trust level 4

	Features		Features
Product Class	Digital	Origin Country	World Wide
Quantity Left	Unlimited	Ships to	World Wide
Ends In	Never	Payment	Escrow

default - 1 day - USD + 0.00

Purchase price: USD 6.60

Qty: 1

0.000797 BTC / 0.116077 LTC / 0.124714 XMR

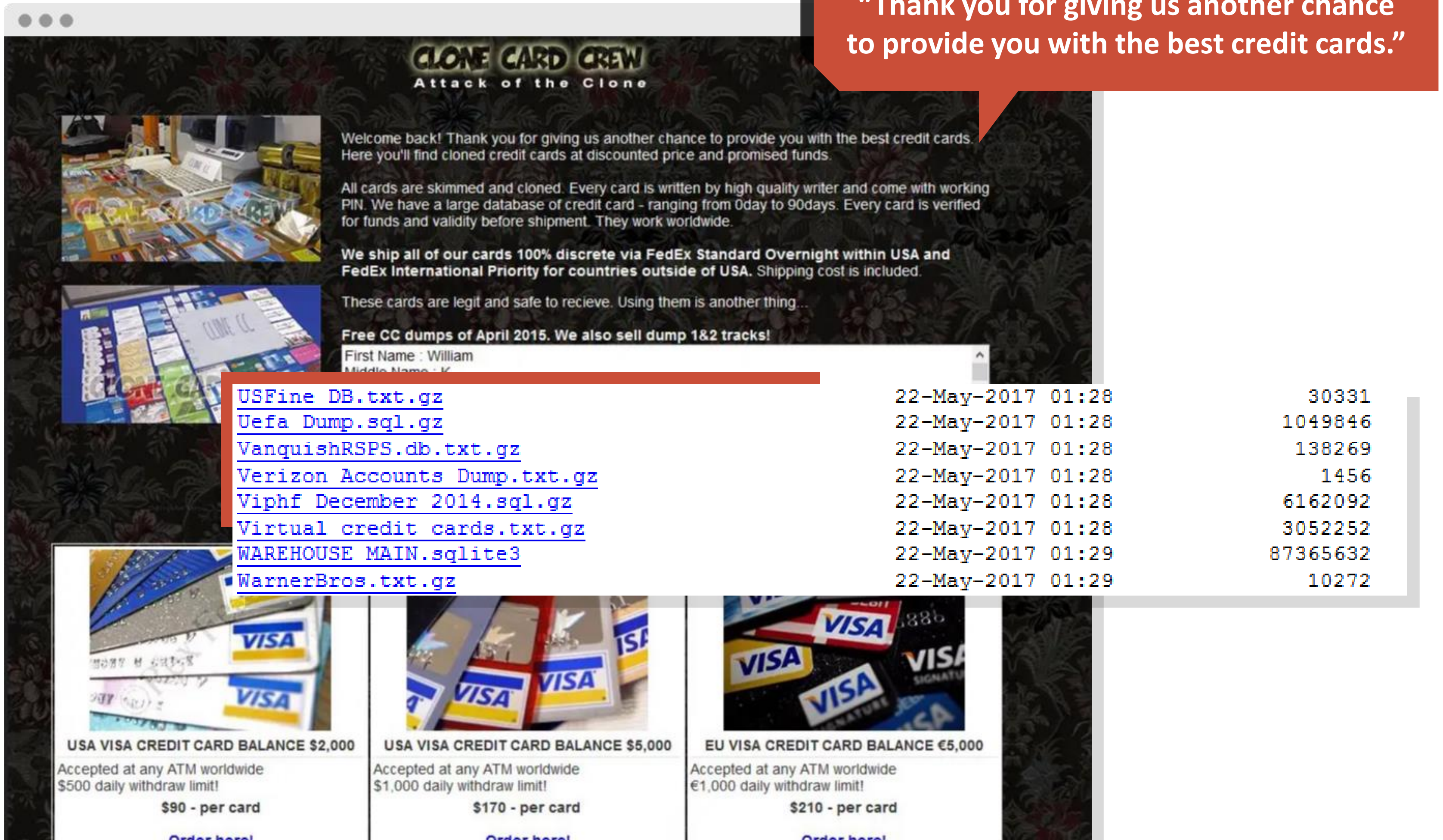
German ID both sides valid

German ID both sides, valid.

You can choose male or female.

SNAPSHOTS FROM THE DARK WEB

"Thank you for giving us another chance to provide you with the best credit cards."



Welcome back! Thank you for giving us another chance to provide you with the best credit cards. Here you'll find cloned credit cards at discounted price and promised funds.

All cards are skimmed and cloned. Every card is written by high quality writer and come with working PIN. We have a large database of credit card - ranging from 0day to 90days. Every card is verified for funds and validity before shipment. They work worldwide.

We ship all of our cards 100% discrete via FedEx Standard Overnight within USA and FedEx International Priority for countries outside of USA. Shipping cost is included.

These cards are legit and safe to recieve. Using them is another thing...

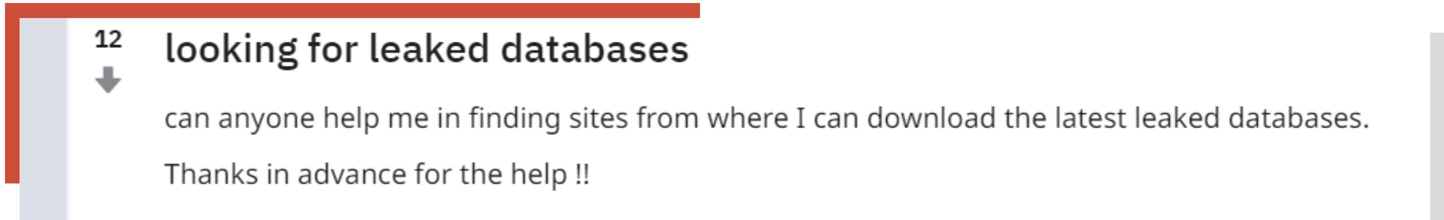
Free CC dumps of April 2015. We also sell dump 1&2 tracks!

First Name : William
Middle Name : K

```
USFine DB.txt.gz                                 22-May-2017 01:28          30331
Uefa Dump.sql.gz                                 22-May-2017 01:28        1049846
VanquishRSPS.db.txt.gz                           22-May-2017 01:28         138269
Verizon Accounts Dump.txt.gz                     22-May-2017 01:28           1456
Viphf December 2014.sql.gz                       22-May-2017 01:28        6162092
Virtual credit cards.txt.gz                      22-May-2017 01:28        3052252
WAREHOUSE MAIN.sqlite3                           22-May-2017 01:29       87365632
WarnerBros.txt.gz                                22-May-2017 01:29          10272
```

USA VISA CREDIT CARD BALANCE $2,000	USA VISA CREDIT CARD BALANCE $5,000	EU VISA CREDIT CARD BALANCE €5,000
Accepted at any ATM worldwide $500 daily withdraw limit!	Accepted at any ATM worldwide $1,000 daily withdraw limit!	Accepted at any ATM worldwide €1,000 daily withdraw limit!
$90 - per card	**$170 - per card**	**$210 - per card**
Order here!	Order here!	Order here!

SNAPSHOTS FROM THE DARK WEB

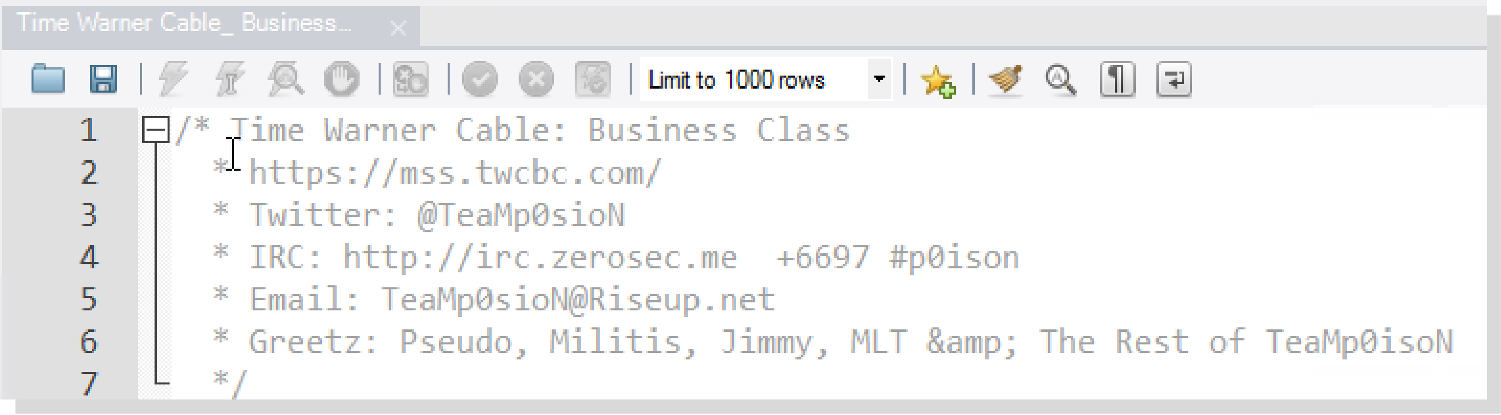


12

looking for leaked databases

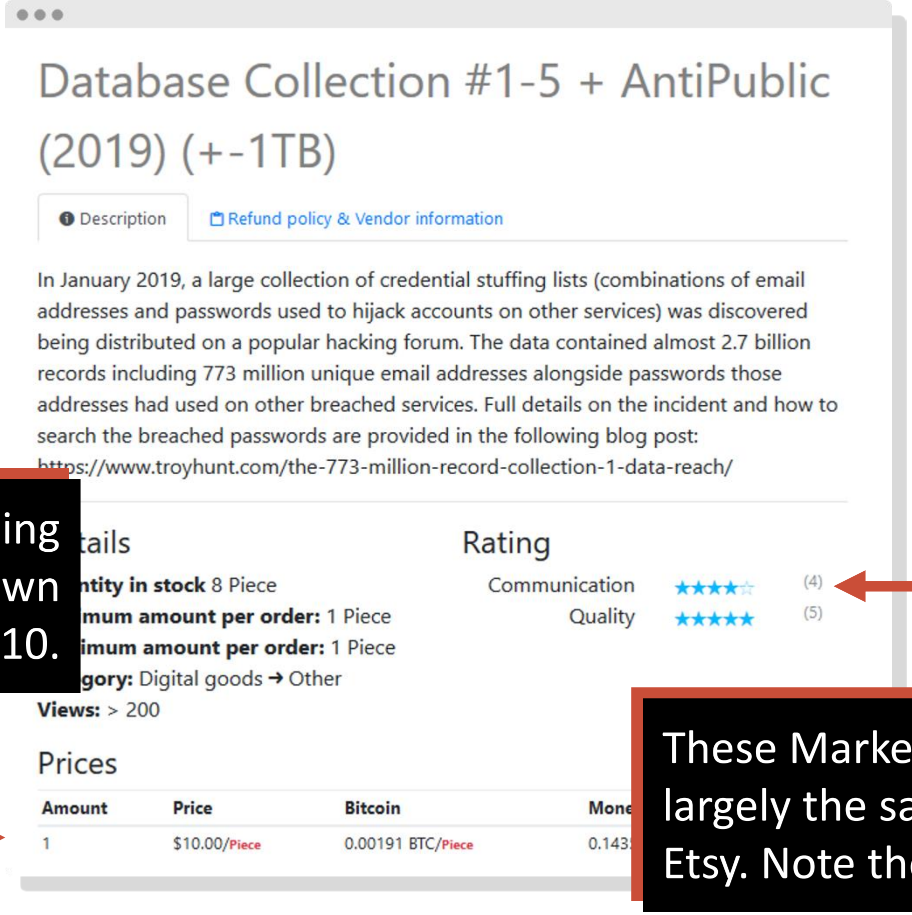
can anyone help me in finding sites from where I can download the latest leaked databases.

Thanks in advance for the help !!



```
/* Time Warner Cable: Business Class
 * https://mss.twcbc.com/
 * Twitter: @TeaMp0sioN
 * IRC: http://irc.zerosec.me  +6697 #p0ison
 * Email: TeaMp0sioN@Riseup.net
 * Greetz: Pseudo, Militis, Jimmy, MLT &amp; The Rest of TeaMp0isoN
 */
```

SNAPSHOTS FROM THE DARK WEB



Database Collection #1-5 + AntiPublic (2019) (+-1TB)

In January 2019, a large collection of credential stuffing lists (combinations of email addresses and passwords used to hijack accounts on other services) was discovered being distributed on a popular hacking forum. The data contained almost 2.7 billion records including 773 million unique email addresses alongside passwords those addresses had used on other breached services. Full details on the incident and how to search the breached passwords are provided in the following blog post: https://www.troyhunt.com/the-773-million-record-collection-1-data-reach/

tails

ntity in stock 8 Piece
mum amount per order: 1 Piece
imum amount per order: 1 Piece
gory: Digital goods → Other
Views: > 200

Rating

Communication	★★★★☆	(4)
Quality	★★★★★	(5)

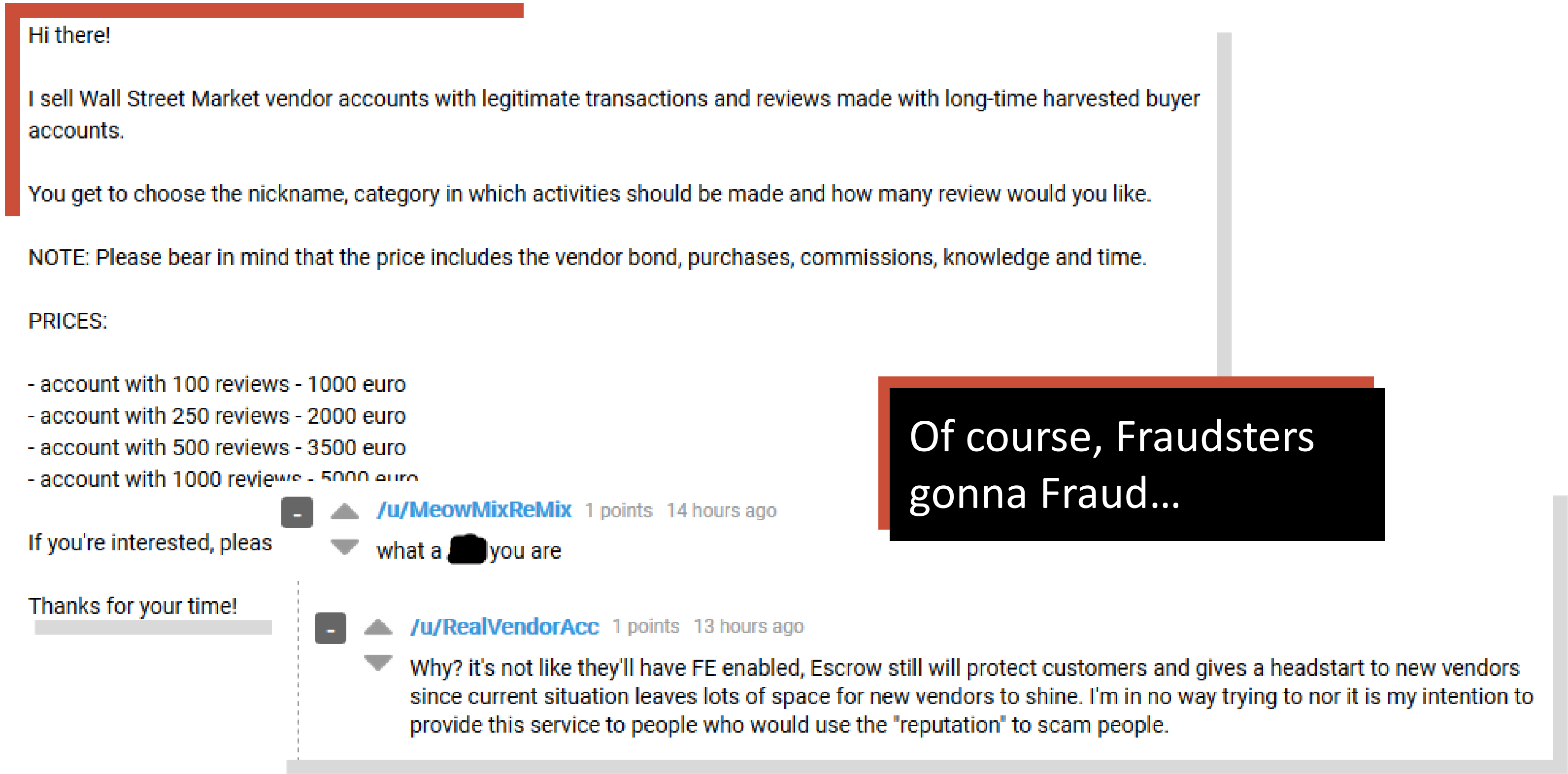
Prices

Amount	Price	Bitcoin	Mone
1	$10.00/Piece	0.00191 BTC/Piece	0.143

Here's someone selling the "largest" known data dump for $10.

These Markets are run largely the same as Ebay or Etsy. Note the Seller ratings.

SNAPSHOTS FROM THE DARK WEB



Hi there!

I sell Wall Street Market vendor accounts with legitimate transactions and reviews made with long-time harvested buyer accounts.

You get to choose the nickname, category in which activities should be made and how many review would you like.

NOTE: Please bear in mind that the price includes the vendor bond, purchases, commissions, knowledge and time.

PRICES:

- account with 100 reviews - 1000 euro
- account with 250 reviews - 2000 euro
- account with 500 reviews - 3500 euro
- account with 1000 reviews - 5000 euro

If you're interested, pleas

Thanks for your time!

/u/MeowMixReMix 1 points 14 hours ago

what a [redacted] you are

/u/RealVendorAcc 1 points 13 hours ago

Why? it's not like they'll have FE enabled, Escrow still will protect customers and gives a headstart to new vendors since current situation leaves lots of space for new vendors to shine. I'm in no way trying to nor it is my intention to provide this service to people who would use the "reputation" to scam people.

Of course, Fraudsters gonna Fraud…

LOOKING FOR A JOB?

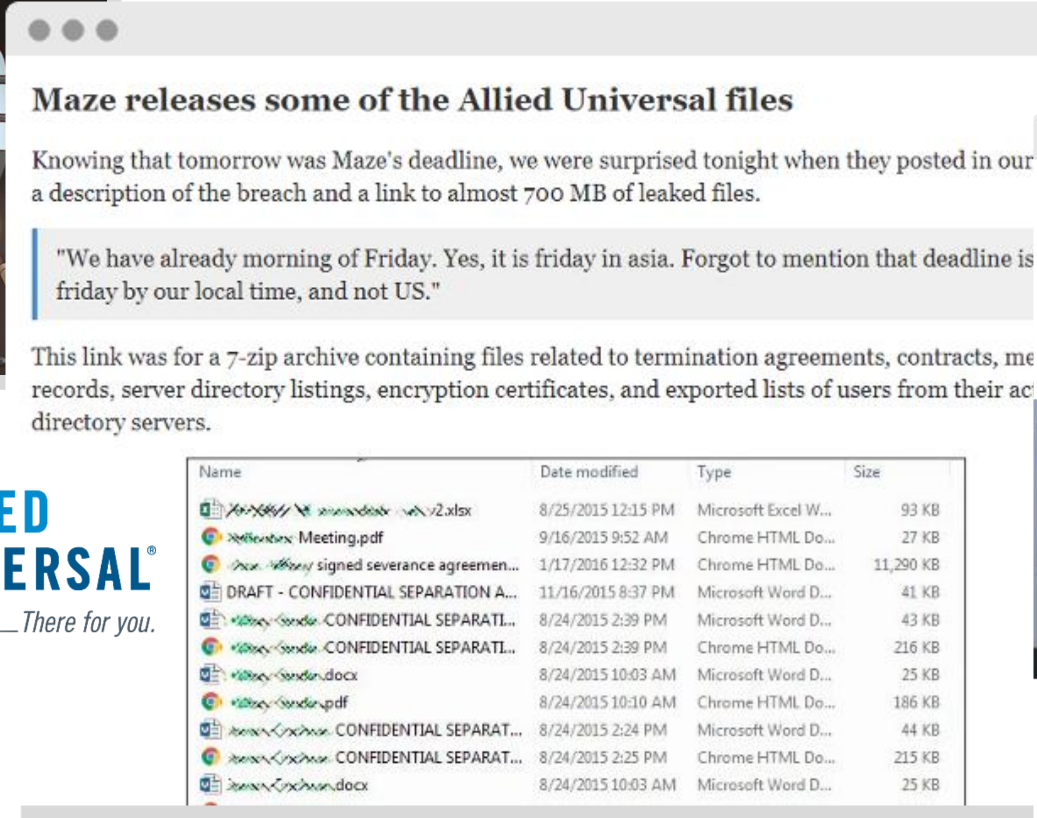
The Dark Overlord is hiring ‘goal oriented’ cybercriminals for $63k/month!

THE DARK WEB IS REAL

The Dark Overlord is hiring. Specifically, it’s hiring software designers and systems engineers with at least “10 years of experience” to “bring innovative approaches to operations and think outside the box.”

An annual salary of $762k (payable after a 90-day probationary period, naturally) with an expected increase to $1.068m after 2 years (contingent upon positive performance reviews, of course).

FROM RANSOMWARE TO PUBLIC EXTORTION



Maze releases some of the Allied Universal files

Knowing that tomorrow was Maze's deadline, we were surprised tonight when they posted in our
a description of the breach and a link to almost 700 MB of leaked files.

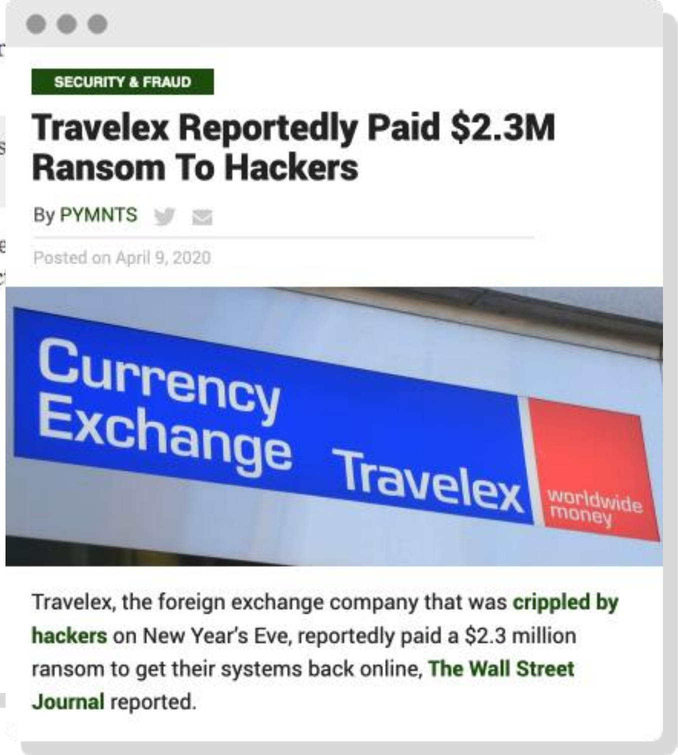
> "We have already morning of Friday. Yes, it is friday in asia. Forgot to mention that deadline is
> friday by our local time, and not US."

This link was for a 7-zip archive containing files related to termination agreements, contracts, me
records, server directory listings, encryption certificates, and exported lists of users from their ac
directory servers.

Name	Date modified	Type	Size
[redacted] v2.xlsx	8/25/2015 12:15 PM	Microsoft Excel W...	93 KB
[redacted] Meeting.pdf	9/16/2015 9:52 AM	Chrome HTML Do...	27 KB
[redacted] signed severance agreemen...	1/17/2016 12:32 PM	Chrome HTML Do...	11,290 KB
DRAFT - CONFIDENTIAL SEPARATION A...	11/16/2015 8:37 PM	Microsoft Word D...	41 KB
[redacted] CONFIDENTIAL SEPARATI...	8/24/2015 2:39 PM	Microsoft Word D...	43 KB
[redacted] CONFIDENTIAL SEPARATI...	8/24/2015 2:39 PM	Chrome HTML Do...	216 KB
[redacted].docx	8/24/2015 10:03 AM	Microsoft Word D...	25 KB
[redacted].pdf	8/24/2015 10:10 AM	Chrome HTML Do...	186 KB
[redacted] CONFIDENTIAL SEPARAT...	8/24/2015 2:24 PM	Microsoft Word D...	44 KB
[redacted] CONFIDENTIAL SEPARAT...	8/24/2015 2:25 PM	Chrome HTML Do...	215 KB
[redacted].docx	8/24/2015 10:03 AM	Microsoft Word D...	25 KB

ALLIED UNIVERSAL®

There for you.



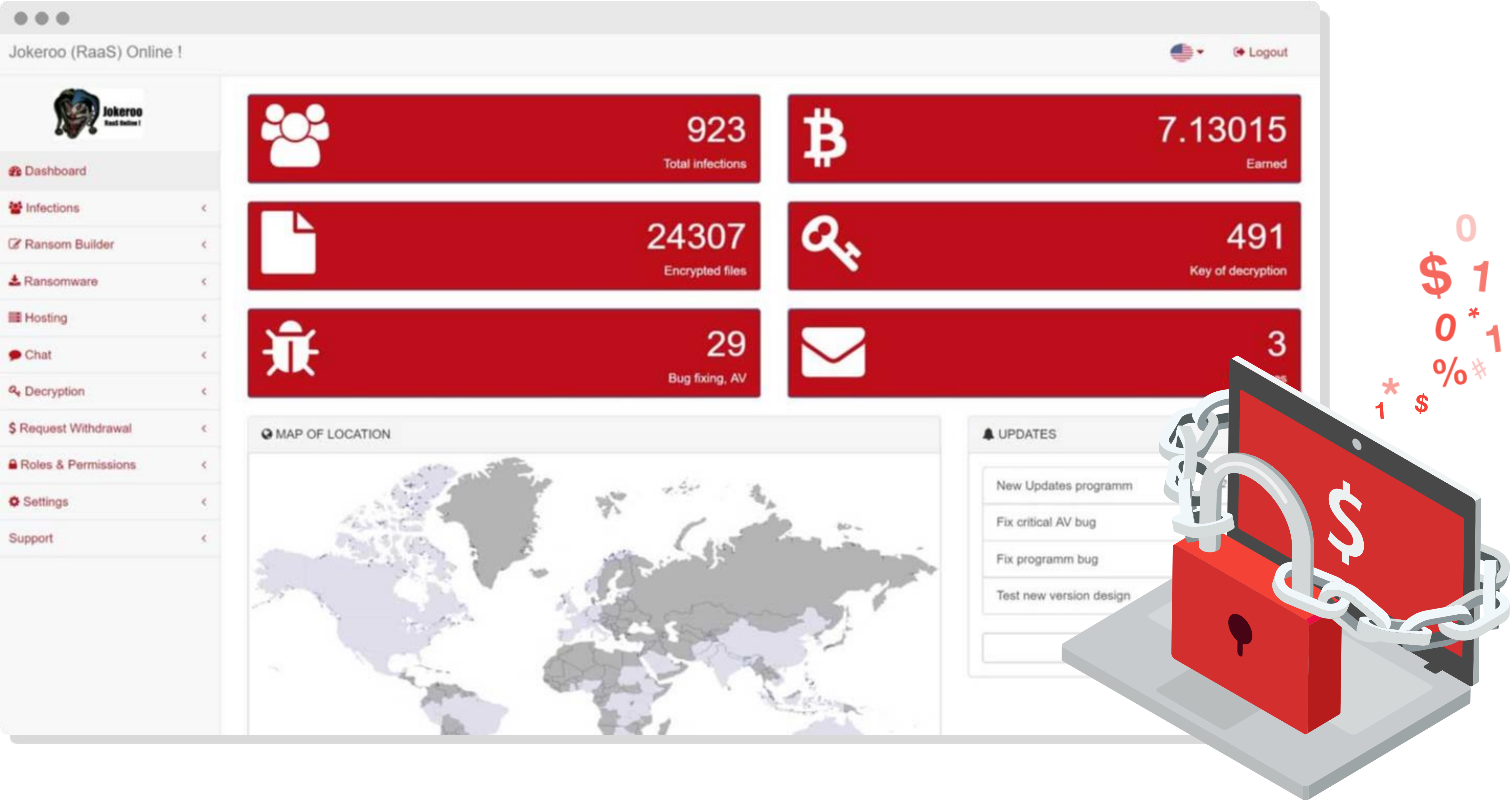
SECURITY & FRAUD

Travelex Reportedly Paid $2.3M Ransom To Hackers

By PYMNTS

Posted on April 9, 2020

Travelex, the foreign exchange company that was **crippled by hackers** on New Year's Eve, reportedly paid a $2.3 million ransom to get their systems back online, **The Wall Street Journal** reported.



Jokeroo (RaaS) Online !

Logout

- Dashboard
- Infections
- Ransom Builder
- Ransomware
- Hosting
- Chat
- Decryption
- $ Request Withdrawal
- Roles & Permissions
- Settings
- Support

923
Total infections

7.13015
Earned

24307
Encrypted files

491
Key of decryption

29
Bug fixing, AV

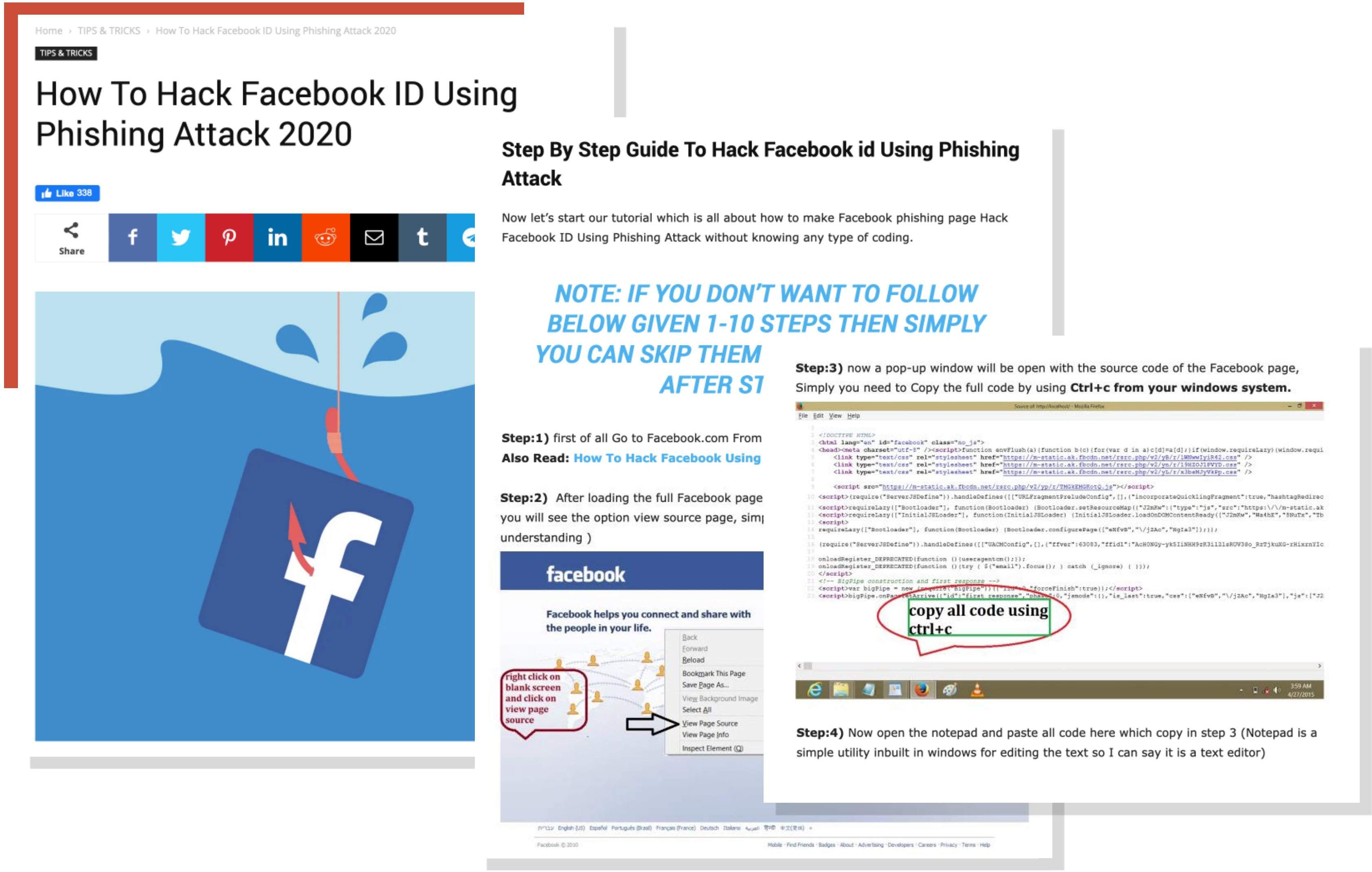
3

MAP OF LOCATION

UPDATES

- New Updates programm
- Fix critical AV bug
- Fix programm bug
- Test new version design

PHISHING KITS: LOOKING FOR A PROJECT?



Home › TIPS & TRICKS › How To Hack Facebook ID Using Phishing Attack 2020

TIPS & TRICKS

How To Hack Facebook ID Using Phishing Attack 2020

Step By Step Guide To Hack Facebook id Using Phishing Attack

Now let's start our tutorial which is all about how to make Facebook phishing page Hack Facebook ID Using Phishing Attack without knowing any type of coding.

NOTE: IF YOU DON'T WANT TO FOLLOW BELOW GIVEN 1-10 STEPS THEN SIMPLY YOU CAN SKIP THEM AFTER ST

Step:1) first of all Go to Facebook.com From

Also Read: How To Hack Facebook Using

Step:2) After loading the full Facebook page you will see the option view source page, simp understanding)

facebook
Facebook helps you connect and share with the people in your life.
Back
Forward
Reload
Bookmark This Page
Save Page As...
View Background Image
Select All
View Page Source
View Page Info
Inspect Element (Q)
right click on blank screen and click on view page source
Facebook © 2010
Mobile · Find Friends · Badges · About · Advertising · Developers · Careers · Privacy · Terms · Help

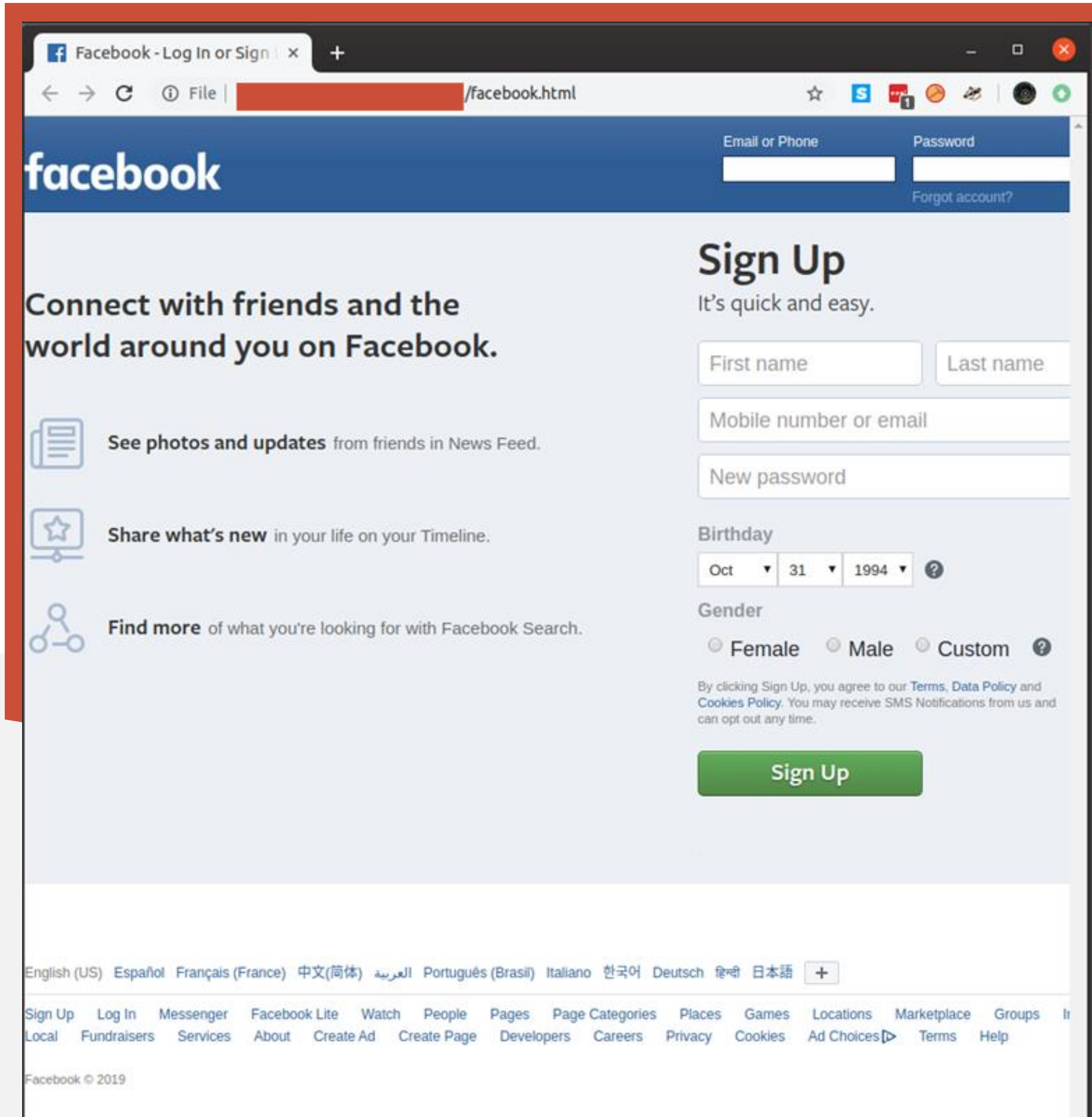
Step:3) now a pop-up window will be open with the source code of the Facebook page, Simply you need to Copy the full code by using **Ctrl+c from your windows system.**

```
<!DOCTYPE HTML>
<html lang="en" id="facebook" class="no_js">
<head><meta charset="utf-8" /><script>function envFlush(a){function b(c){for(var d in a)c[d]=a[d];}if(window.requireLazy){window.requi
    <link type="text/css" rel="stylesheet" href="https://m-static.ak.fbcdn.net/rsrc.php/v2/yB/r/1WNwwIyiR42.css" />
    <link type="text/css" rel="stylesheet" href="https://m-static.ak.fbcdn.net/rsrc.php/v2/yn/r/19HZOJ1PVYD.css" />
    <link type="text/css" rel="stylesheet" href="https://m-static.ak.fbcdn.net/rsrc.php/v2/yL/r/x3bsMJyVkPp.css" />

    <script src="https://m-static.ak.fbcdn.net/rsrc.php/v2/yp/r/TMGkEMGRotQ.js"></script>
<script>(require("ServerJSDefine")).handleDefines([["URLFragmentPreludeConfig",[],{"incorporateQuicklingFragment":true,"hashtagRedirec
<script>requireLazy(["Bootloader"], function(Bootloader) {Bootloader.setResourceMap({"J2mKw":{"type":"js","src":"https:\/\/m-static.ak
<script>requireLazy(["InitialJSLoader"], function(InitialJSLoader) {InitialJSLoader.loadOnDOMContentReady(["J2mKw","Wa4hE","8NuTx","Tb
<script>
requireLazy(["Bootloader"], function(Bootloader) {Bootloader.configurePage(["eNfvB","\/jZAc","HgIa3"]);});

(require("ServerJSDefine")).handleDefines([["UACMConfig",[],{"ffver":63083,"ffid1":"AcHONGy-ykSIiNHH9zK3i121sRUV38o_RzTjkuXG-rHixrnYIc

onloadRegister_DEPRECATED(function (){useragentcm();});
onloadRegister_DEPRECATED(function (){try { $("email").focus(); } catch (_ignore) { }});
</script>
<!-- BigPipe construction and first response -->
<script>var bigPipe = new (require("BigPipe"))({"lid":0,"forceFinish":true});</script>
<script>bigPipe.onPageletArrive({"id":"first_response","phase":0,"jsmods":{},"is_last":true,"css":["eNfvB","\/jZAc","HgIa3"],"js":["J2
```

Step:4) Now open the notepad and paste all code here which copy in step 3 (Notepad is a simple utility inbuilt in windows for editing the text so I can say it is a text editor)

STEP-BY-STEP GUIDES TO BUILDING YOUR OWN

PHISHING KITS: LOOKING FOR A PROJECT?



Facebook - Log In or Sign

File | [redacted]/facebook.html

facebook

Email or Phone

Password

Forgot account?

Connect with friends and the world around you on Facebook.

See photos and updates from friends in News Feed.

Share what's new in your life on your Timeline.

Find more of what you're looking for with Facebook Search.

Sign Up

It's quick and easy.

First name

Last name

Mobile number or email

New password

Birthday

Oct ▾ 31 ▾ 1994 ▾ ?

Gender

○ Female ○ Male ○ Custom ?

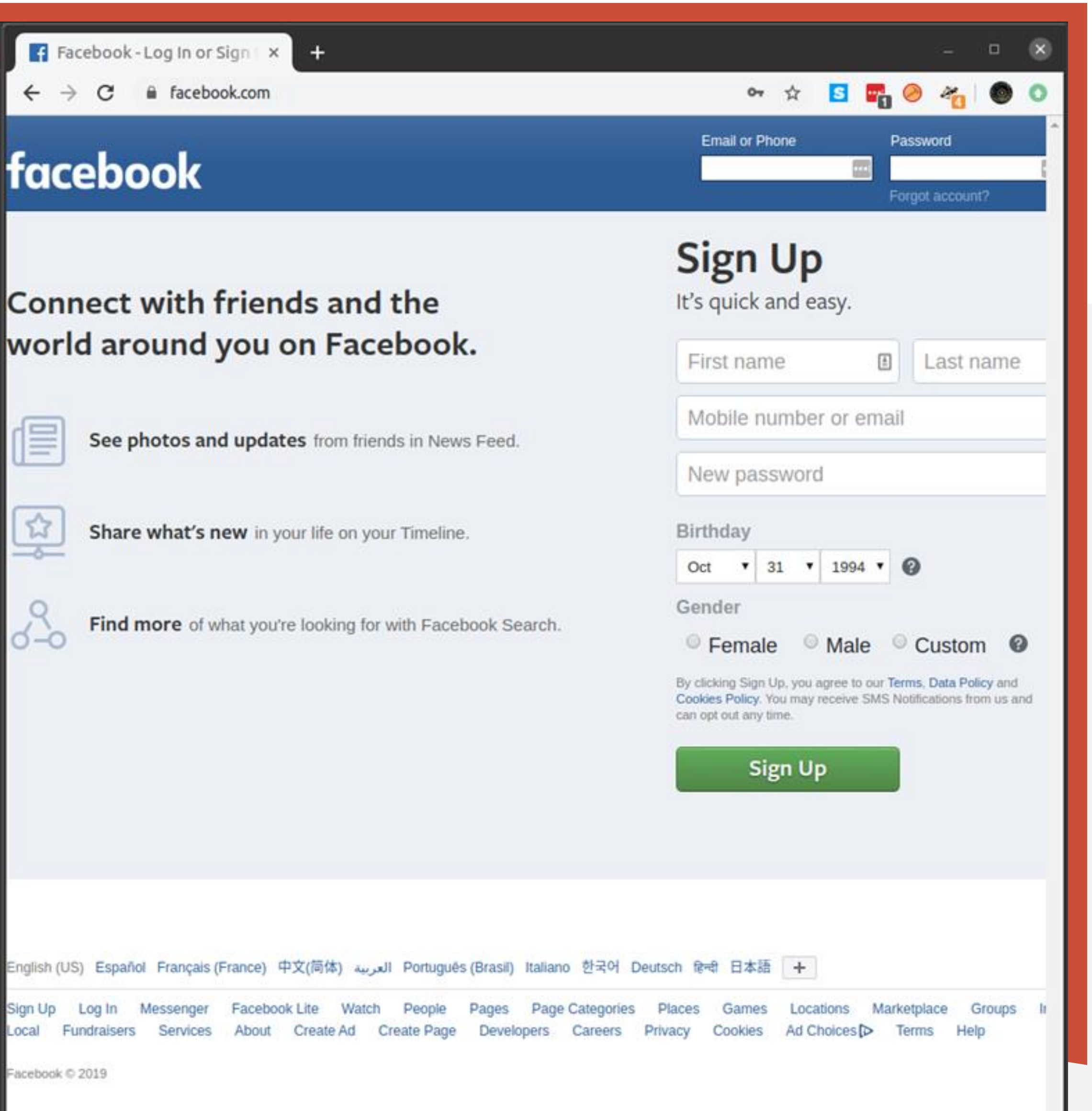
By clicking Sign Up, you agree to our Terms, Data Policy and Cookies Policy. You may receive SMS Notifications from us and can opt out any time.

Sign Up

English (US) Español Français (France) 中文(简体) العربية Português (Brasil) Italiano 한국어 Deutsch हिन्दी 日本語 +

Sign Up Log In Messenger Facebook Lite Watch People Pages Page Categories Places Games Locations Marketplace Groups I
Local Fundraisers Services About Create Ad Create Page Developers Careers Privacy Cookies Ad Choices ▷ Terms Help

Facebook © 2019



Facebook - Log In or Sign

facebook.com

facebook

Email or Phone

Password

Forgot account?

Connect with friends and the world around you on Facebook.

See photos and updates from friends in News Feed.

Share what's new in your life on your Timeline.

Find more of what you're looking for with Facebook Search.

Sign Up

It's quick and easy.

First name

Last name

Mobile number or email

New password

Birthday

Oct ▾ 31 ▾ 1994 ▾ ?

Gender

○ Female ○ Male ○ Custom ?

By clicking Sign Up, you agree to our Terms, Data Policy and Cookies Policy. You may receive SMS Notifications from us and can opt out any time.

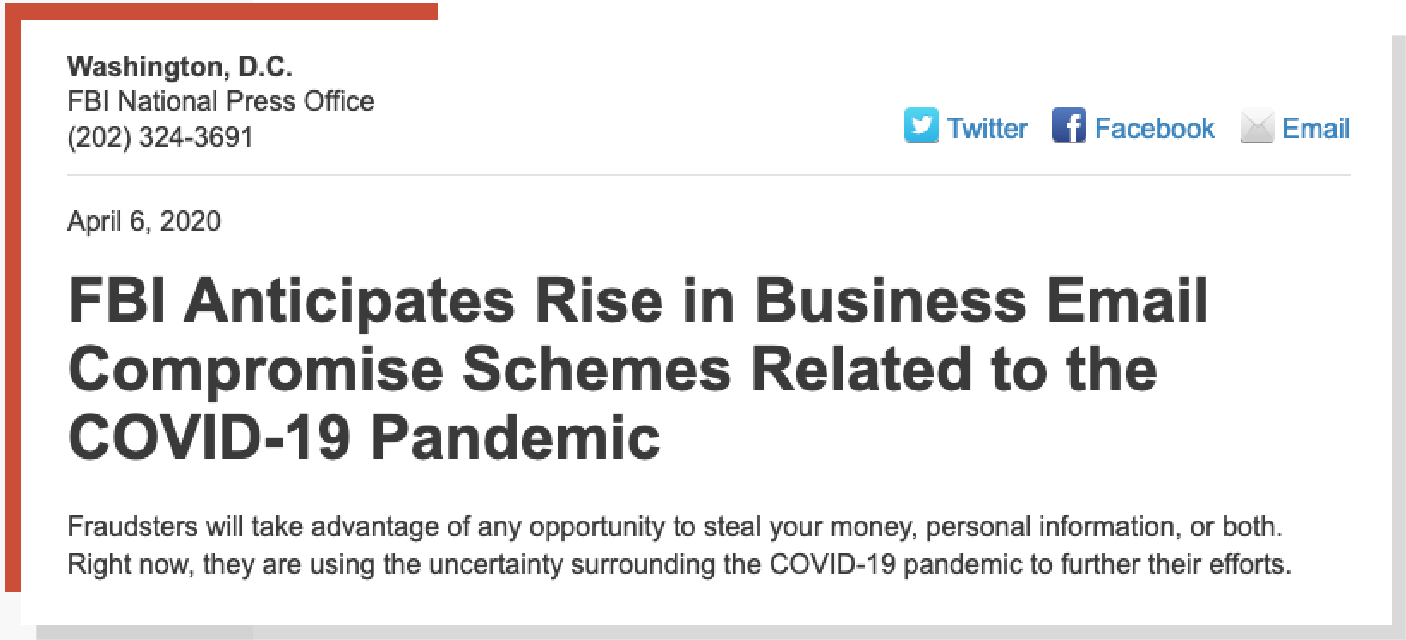
Sign Up

English (US) Español Français (France) 中文(简体) العربية Português (Brasil) Italiano 한국어 Deutsch हिन्दी 日本語 +

Sign Up Log In Messenger Facebook Lite Watch People Pages Page Categories Places Games Locations Marketplace Groups I
Local Fundraisers Services About Create Ad Create Page Developers Careers Privacy Cookies Ad Choices ▷ Terms Help

Facebook © 2019

PHISHING ATTACKS ARE SURGING!



Washington, D.C.
FBI National Press Office
(202) 324-3691

Twitter Facebook Email

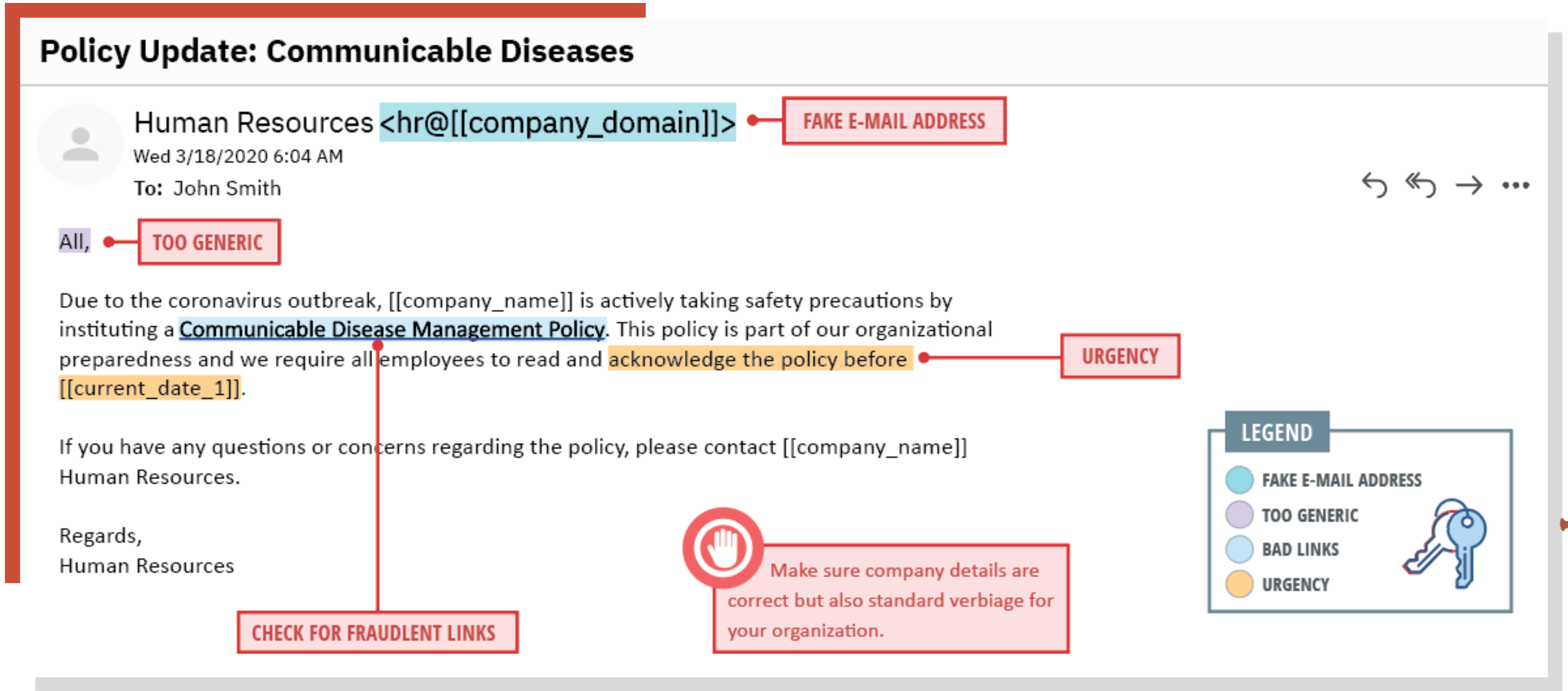
April 6, 2020

FBI Anticipates Rise in Business Email Compromise Schemes Related to the COVID-19 Pandemic

Fraudsters will take advantage of any opportunity to steal your money, personal information, or both. Right now, they are using the uncertainty surrounding the COVID-19 pandemic to further their efforts.

PHISHING ATTACKS ARE SURGING!

COVID-19 Examples



Policy Update: Communicable Diseases

Human Resources <hr@[[company_domain]]>
Wed 3/18/2020 6:04 AM
To: John Smith

All,

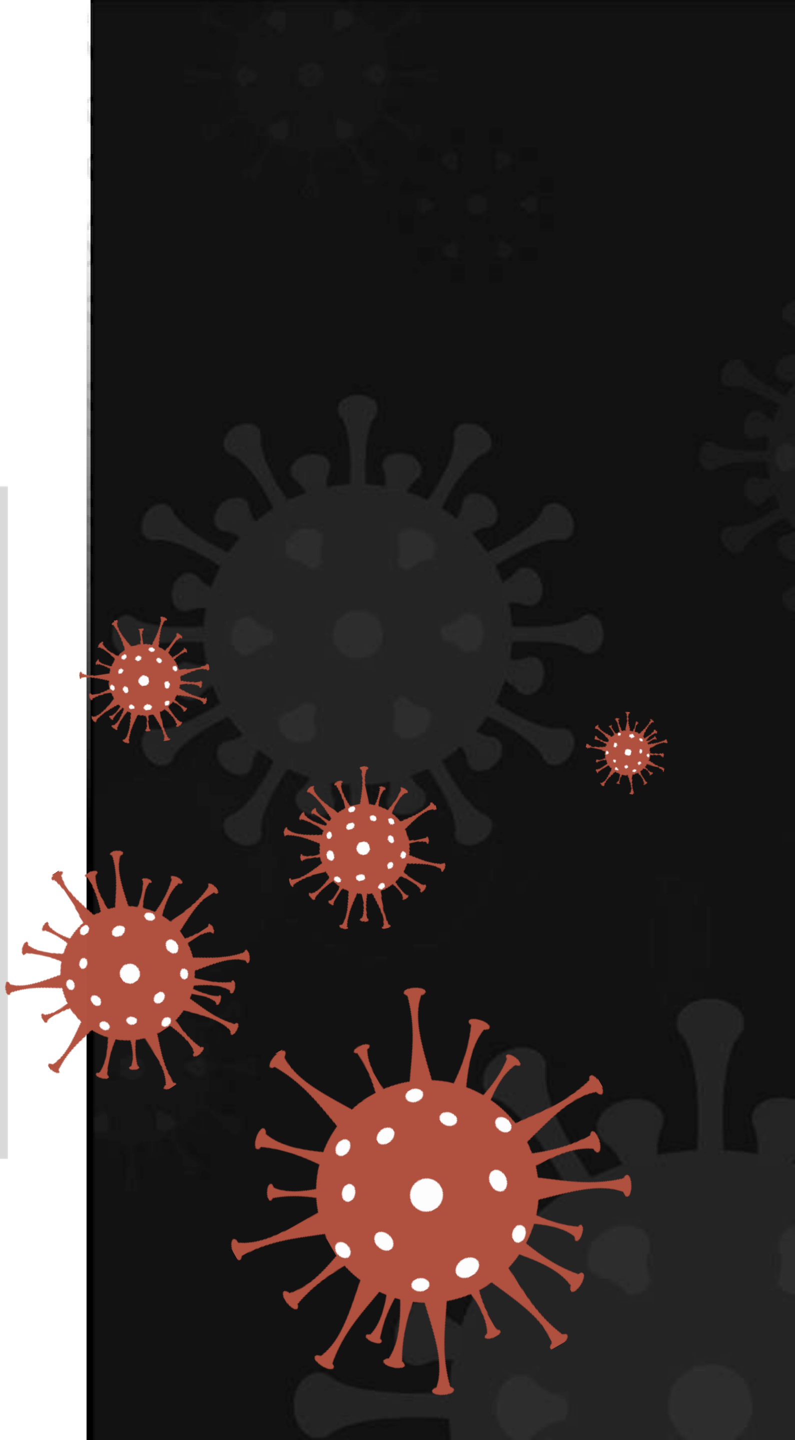
Due to the coronavirus outbreak, [[company_name]] is actively taking safety precautions by instituting a Communicable Disease Management Policy. This policy is part of our organizational preparedness and we require all employees to read and acknowledge the policy before [[current_date_1]].

If you have any questions or concerns regarding the policy, please contact [[company_name]] Human Resources.

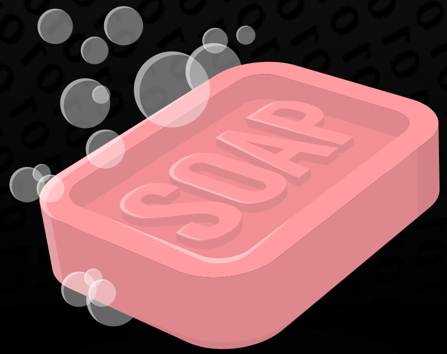
Regards,
Human Resources

Make sure company details are correct but also standard verbiage for your organization.

LEGEND
- ● FAKE E-MAIL ADDRESS
- ● TOO GENERIC
- ● BAD LINKS
- ● URGENCY



GOOD EMAIL HYGIENE



The CDC recommends you take at least 20 seconds to wash your hands to avoid germs. We recommend you take at least 20 seconds to review each email to avoid falling victim to a phishing scam.

1 **WATCH FOR OVERLY GENERIC CONTENT AND GREETINGS**
Cyber criminals will send a large batch of emails. Look for examples like “Dear valued customer.”

2 **EXAMINE THE ENTIRE EMAIL ADDRESS**
The first part of the email address may be legitimate, but the last part might be off by letter or may include a number in the usual domain.

3 **LOOK FOR URGENCY OR DEMANDING ACTIONS**
“You’ve won! Click here to redeem prize,” or “We have your browser history pay now or we are telling your boss.”

4 **CAREFULLY CHECK ALL LINKS**
Mouse over the link and see if the destination matches where the email implies you will be taken.

5 **NOTICE MISSPELLINGS, INCORRECT GRAMMAR, & ODD PHRASING**
This might be a deliberate attempt to try to bypass spam filters.

6 **CHECK FOR SECURE WEBSITES**
Any webpage where you enter personal information should have a url with https://. The “s” stands for secure.

7 **DON’T CLICK ON ATTACHMENTS RIGHT AWAY**
Attachments containing viruses might have an intriguing message encouraging you to open them such as “Here is the Schedule I promised.”

PROTECT YOUR EMPLOYEES

10 TIPS

TO KEEP CYBERCRIMINALS OUT WHILE CORONAVIRUS KEEPS YOU IN

Get the facts 1

Stay away from the rumor mill and use Information from reliable sources to make business decisions in chaotic times.

Think twice before clicking links 2

Make sure staffers are on the lookout for suspicious links that can lead to ransomware.

Be suspicious of expected attachments 3

Ensure users only open attachments from proven, trusted sources no matter how ‘official’ that attachment looks.

Automate compliance 4

Have one less thing to worry about by choosing a dynamic web portal system that keeps track of everything.

Protect those passwords 5

Encourage safe password practices like using a password manager and not writing them on sticky notes.

6 Beware of strange networks

Make staffers aware of the dangers of logging in from unsecured public and home WiFi networks and how to use them safely.

7 Use two-factor authentication

An extra layer of security keeps passwords and data safe.

8 Keep an eye on the bad guys

Monitor the Dark Web to watch for company data so a problem can be addressed before it becomes a crisis.

9 Stay current on the threats

Work with a responsive partner that’s on top of today’s challenges.

10 Ask for help

Consult a security expert to plan effective strategies and get innovated solutions.

Incident Response
FORENSIC & CYBER

Thank you

Campbell McKenzie
0800 WITNESS
021 779 310
campbell@incidentresponse.co.nz
incidentresponse.co.nz

We help you Prepare, Respond and Recover from Forensic and Cyber Incidents