Hacking law firms with abandoned domain names

“You had better keep your expiring domain names alive”

gabor:~$ **whoami**

Gabor Szathmari

@gszathmari

Cyber security expert @ Iron Bastion
Privacy advocate @ CryptoAUSTRALIA

Which one is real?

OptusGames.com.au

TheWestPacCentre.com.au

wmWoolworthsMoneyCreditCard.com.au

@gszathmari

Gabor Szathmari
@gszathmari

I want to play a game. Which previously expired domain is available for registration again (and was belonging to the corresponding firm)?

The third option is wmwoolworthsmoneycreditcard[.]com[.]au

#security @sectalks @Optus @Westpac @woolworths

0% optusgames.com.au

0% thewestpaccentre.com.au

0% wmwoolworth...card.com.au

Overview

- How domain names die?
- How to find good domain names?
- Hacking law firms – The examples
- Tips for individuals & red/blue teams

Let’s go!

How domain names die?

.au domain lapsing:

1. Active
2. ‘Expired Hold’ (30 days)
3. ‘Expired Pending Purge’ (1 day)
4. Purged at 1.00pm (AEST)
5. Available for new registration

Official Domain Name Drop List

The Domain Name Drop List shows the date and time that Domain Names are eligible to be purged. When a Domain Name is purged, it becomes available for registration according to the policy of the Regulator. Unless restored the Domain Name will be purged at the next Purge Cycle, also as defined in Regulator Policy. The Purge Cycle is an automated process within the Domain Name Registry System.

Please note the date and time associated with the Domain Name in the lists below are represented in Universal Coordinated Time (UTC).

Expired Domain Names

This list shows Domain Names which have passed through the Expiry Process in the Domain Name Registry System and are eligible to be purged. These Domain Names generally cannot be recovered and will purge at the next cycle that occurs NO EARLIER THAN the date and eligible purge time (1:00pm AEST) listed in the report below.

Expired Domains Report

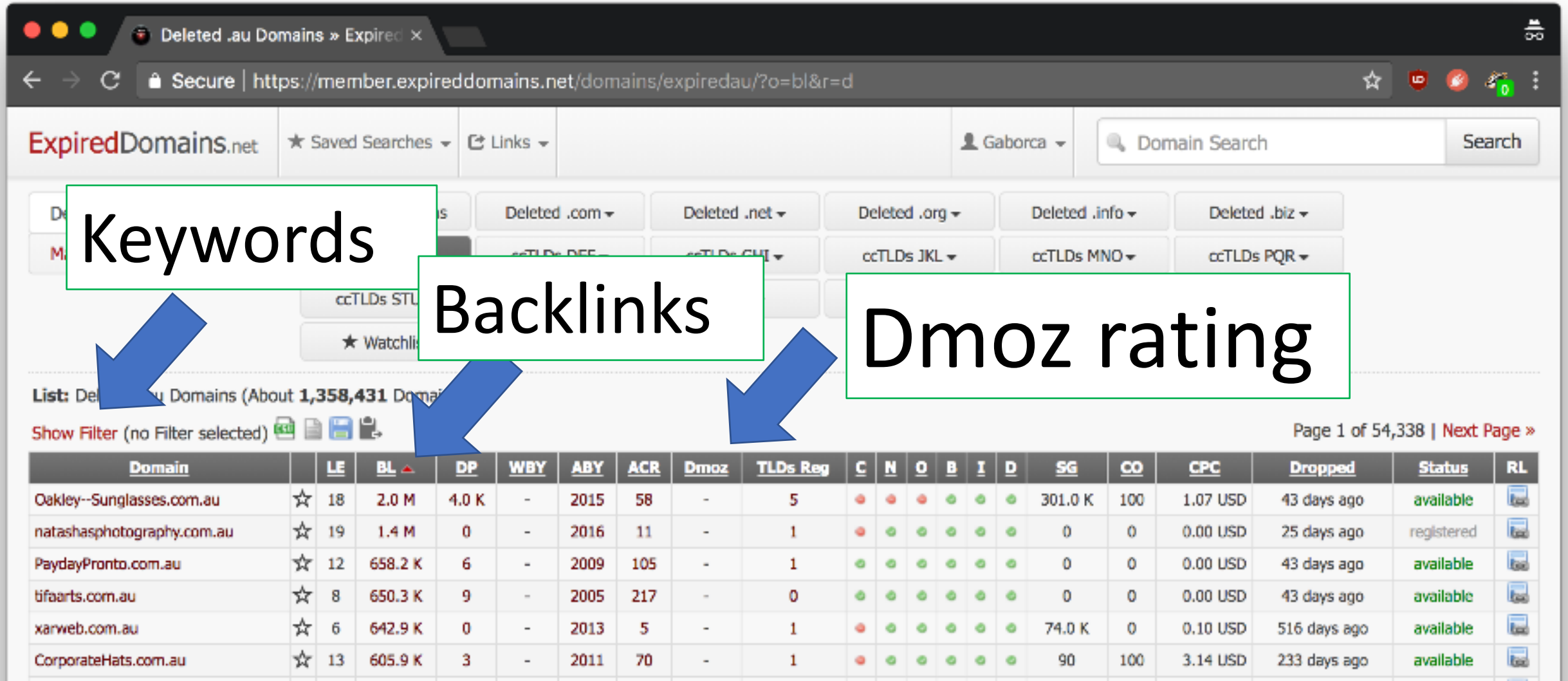
How to find good domain names?

The manual method 1.

$ cat RO_expired-domain-names_au_daily_2018-09-08.csv | **grep law**

2018-09-04,04:13:42,joshlawelectrical.com.au
2018-09-04,04:30:04,comslaw.org.au
2018-09-04,05:37:05,lawyersforbusiness.net.au
[…]

The manual method 2.



Domain		LE	BL	DP	WBY	ABY	ACR	Dmoz	TLDs Reg	C	N	O	B	I	D	SG	CO	CPC	Dropped	Status	RL
Oakley--Sunglasses.com.au	☆	18	2.0 M	4.0 K	-	2015	58	-	5							301.0 K	100	1.07 USD	43 days ago	available	
natashasphotography.com.au	☆	19	1.4 M	0	-	2016	11	-	1							0	0	0.00 USD	25 days ago	registered	
PaydayPronto.com.au	☆	12	658.2 K	6	-	2009	105	-	1							0	0	0.00 USD	43 days ago	available	
tifaarts.com.au	☆	8	650.3 K	9	-	2005	217	-	0							0	0	0.00 USD	43 days ago	available	
xarweb.com.au	☆	6	642.9 K	0	-	2013	5	-	1							74.0 K	0	0.10 USD	516 days ago	available	
CorporateHats.com.au	☆	13	605.9 K	3	-	2011	70	-	1							90	100	3.14 USD	233 days ago	available	

Workflow

1. **Identify good sounding names**
2. **How the website looked like?** → web.archive.org
3. **Look up domain reputation**
   (for proxy and spam filter bypass)
4. **Backlinks** (DMoz / Ahrefs)
5. **Register domain**
6. **Profit!**

Hacking law firms with abandoned domains

Reasons to target law firms

- Merge and get acquired frequently
- Low-security businesses
- Manage sensitive data and high-value payments

Reasons to NOT target law firms

#1: Tendency to sue people

What we did

1. Identified valuable expired domain names
2. Registered domain name
3. Added our MX hosts – ‘catch all’
4. Started receiving emails

Question 1.

What are the auDA requirements to register a **.com.au** domain?

Question 1.

1. Must be one of these:
   - Registered business
   - Sole trader
   - Incorporated association
   - Trade mark owner
2. Must provide ABN/ACN/ARBN/TM#
3. Be able to tick a box

.COM.AU Registration Information

Legal Entity:*

Totally Legit Business Pty Ltd

For your .com.au name(s)

Entity Type:*

Company

What best describes mydomain333.com.au: : *

- (•) **This domain is closely and substantially connected to my organization or activities undertaken by my organization.**
- ( ) **This domain name is an exact match, an acronym or abbre of my company or trading name, organization or association name or trademark.**

Identification Type:* ABN (6–11 characters)

Identification Number:* 123456

☑ **Application Agreement***

By submitting this application, you represent and warrant that: (a) all information provided to register or renew the domain name (including all supporting documents, if any) are true, complete and correct, and are not misleading in any way, and the

Order Summary

1 domain(s) pending registration

× MYDOMAIN333.COM.AU

Loot #1: Statements and notifications

From Bankwest <bob.mailbox@bankwest.com.au>

Subject **Bankwest - You have a new credit card eStatement**

To [redacted]

Reply | Reply All | Forward | Archive | Junk | Delete

18/8

bankwest

You have a new credit card eStatemen

Dear [redacted]

A new eStatement for your **Bankwest Lite MasterCard** ending [redacted] s now available.

Simply login to the Bankwest App or Bankwest Online Banking to view, download or print your statement.

Need a payment reminder?
Set up a Bankwest Easy Alert within the Bankwest App to send you a reminder of your statement due date. Visit our website for more information on Bankwest Easy Alerts and the Bankwest App as some device limitations may apply.

Note: You should never click a link in an email to go to Bankwest's site and log in. The link may not be genuine and you might be disclosing confidential access details to a third party. This email is automatically generated; please do not reply as our system will not generate a response. For telephone queries regarding Bankwest Online Banking please contact 1300 440 749.

From National Australia Bank <donotreply-internetbanking@nab.com.au>

Subject **Hi - Your NAB Smart Statements are now available for multiple accounts**

To [redacted]

Reply | Reply All | Forward | Archive | Junk | Delete | More

2/7/18, 00:50

nab

NAB Smart Statement

View, save or print your NAB Smart Statements

Dear Customer

The latest NAB Smart Statement is now available for your accounts ending in:
- 6880
- 9910

To access your NAB Smart Statement in NAB Internet Banking:

From Amazon.com.au <digital-no-reply@amazon.com.au>

Subject **Your Amazon.com.au Order What Alice Forgot.**

To [redacted]

Reply | Reply All | Forward | Archive

amazon.com.au

Your Account | Amazon.com.au

Order Confirmation

Order [redacted]

Hello [redacted]

Thank you for shopping with us. All Kindle content, including books and Kindle active content, that you've purchased from the Kindle Store is stored in your content library on Amazon.com.au.

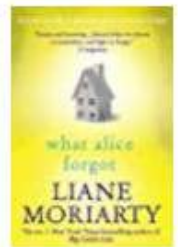
View and manage your books from your content library.

Manage Your Kindle

Order Details

Order [redacted]

Placed on Sunday, August 12, 2018



What Alice Forgot — **$9.99**

Kindle Edition

Sold by Macmillan (AU)

Review this item

Item(s) Subtotal:	$9.99
Order Grand Total:	**$9.99**

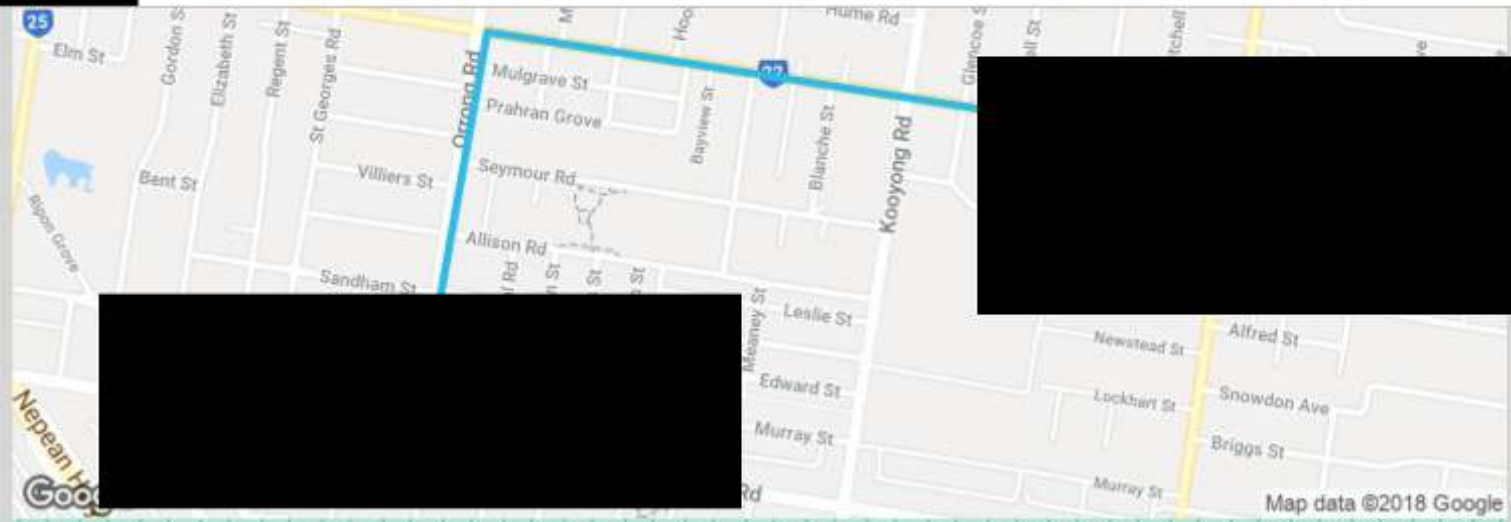
From Uber Receipts <uber.australia@uber.com>

Subject **Your Saturday evening trip with Uber**

To [redacted]

Reply | Reply All | Forward | Archive | Junk | Delete | More

4/8/18, 19



UBER

A$12.96

Thanks for choosing Uber, [redacted]

August 4, 2018 | UberX

[redacted]

From Telstra Mobile Data Usage <mobiledatausage@telstra.com>

Subject **Mobile Data Group Usage Notification from Telstra**

To [redacted]

Reply | Reply All | Forward | Archive | Junk

Mobile Data Usage Notification

Hello,

We wanted to let you know you've used 85% of your 2.60GB included shared data allowance for the mobile service 04[redacted] with 12 days le

Phone number

Keeping you informed

We'll continue to notify you by email once you reach 100% of your monthly shared data allowance even if you've added a Data Pack to your current plan.

From 614[redacted]@optusmobile.com.au

Subject

To [redacted]

Text-to-email service

Hey
Tried to call a few times

[redacted]

Loot #2:
Legal documents

From [redacted]
Subject [redacted]
To [redacted]

Reply | Reply All | Forw

Family legal matter

From: [redacted]
Sent: Tuesday, 1 May 2018 4:42 PM
To: [redacted]
Subject: [redacted]

Dear [redacted]

Please see attached letter from [redacted] to the Court for your records.

Kind regards

[redacted] Accredited Specialist (Family Law) | [redacted]

[redacted]

[redacted]

CC: [redacted]
Sydney NSW
By email to: [redacted]

Family legal matter

Dear List Clerk,

RE: [redacted]

Our client's application for Orders to set aside Orders made by consent by the Local Court at [redacted] under the provisions of s79A of the *Family Law Act 1975* has been listed for Hearing on [redacted]

Pursuant to what we under are the provisions of *Family Law Rule 15.12* we have filed and served our client's updated affidavit sworn [redacted] 2018 but we have not filed the exhibits to this affidavit. Would you please advise whether such exhibits are to be tendered at the commencement of the Hearing on [redacted] 2018 or whether they should be filed at an earlier

[redacted]

TAX INVOICE - [redacted]

Tax invoice

Professional Fees

Date	Description	Fee Earner	Units	Amount (ex. GST)
[redacted]		[redacted]	2	$120.00
			1	$60.00
			1	$60.00
			1	$60.00
			43	$2,580.00
			1	$60.00
Total:			49	$2,940.00

INVOICE SUMMARY

Professional Fees	$2,940.00
GST	$294.00
This Invoice Total (Due in 7 days)	$3,234.00
Outstanding Invoices (Due now)	$10,000.00
Amount we intend to pay from Trust	$0.00
TOTAL AMOUNT DUE	**$13,234.00**

From [redacted]

Subject [redacted] Divorce case

To [redacted]

Cc [redacted]

Client enquiry

Hi [redacted]

Hope you are keeping well.

I don't know if you remember my case of some years ago, but you very kindly fought for me to return to UK with my son [redacted]

You'll be pleased to know that I have settled back in UK with [redacted]

From [redacted]

Subject **FW: Financial Separation Negotiations**

To [redacted]

Reply | Reply All | Forward | Archive | Junk | Delete | More

18:47

Negotiation strategy

Dear [redacted]

I hope this email finds you well …

You will see in your diary that I have booked you for a 1 hour teleconference tomorrow – that should give us enough time for you to get up to speed on what is happening and to help formulate a strategy going forward. [redacted]

[redacted]

I will call your office to discuss. Speak soon.

Regards,

[redacted]

Settlement Offer

I appreciate the position you find yourself and I agree that the situation calls for finalisation of our financial situation to help expedite things.

As regards your proposal, there are omissions regarding both the past and present costs, which need to be addressed.

I am willing to use the principal of a fair and equitable distribution to finalise this matter forthwith.

No lingering uncertainties, therefore I propose.

Settlement

Negotiation strategy

1. **House**
   [redacted]

2. **Companies.**
   [redacted]

[redacted]

nab

NAB Classic Banking
For further information call 13 22 65 for Personal Accounts or 13 10 12 for Business Accounts.

[redacted]

[redacted]

Account Balance Summary

Opening balance	[redacted]
Total credits	
Total debits	
Closing balance	

Statement starts 18 January 2018
Statement ends 17 July 2018

Bank statements

Outlet Details

[redacted]

Account Details

[redacted]

BSB number [redacted]
Account number [redacted]

Lending Investment & Insurance Enquiries

Banker [redacted]
Telephone number

Transaction Details

Date	Particulars	Debits	Credits	Balance
[redacted]	Brought Forward			
	Settlement Surplus		[redacted]	[redacted]

Par-tay! 

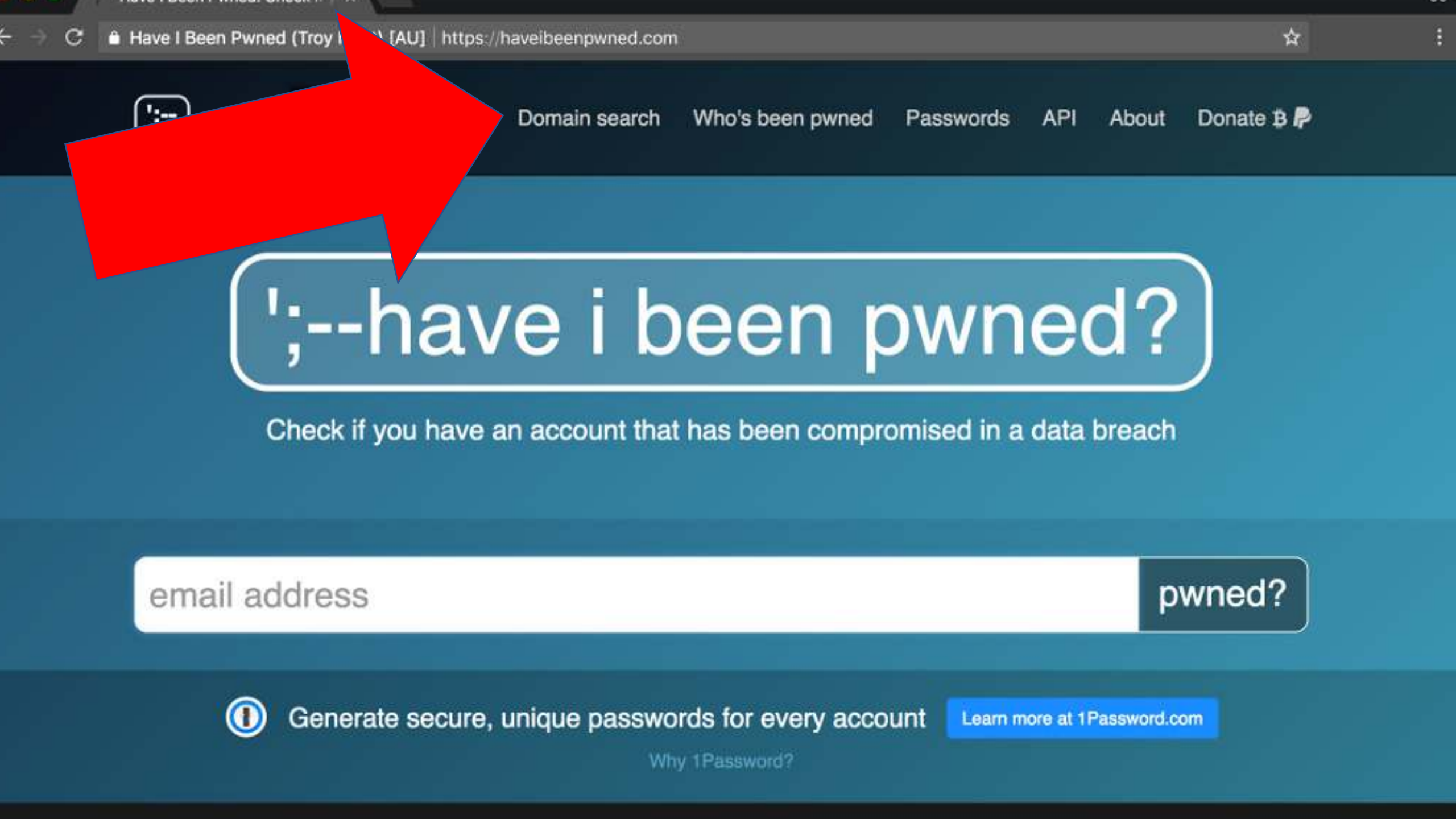
Reply | Reply All | Forward | Archive

From [redacted]
Subject **CBD**
To [redacted]

[redacted]

Good to catch up with you yesterday. Glad I left when I did though as you boys are league ahead of me on the drinking!
Anyway I am free to catch up tomorrow.
Just let me know when and what time works best. [redacted] around in the afternoon as well.
Kind regards,
[redacted]

Loot #3: Password recovery

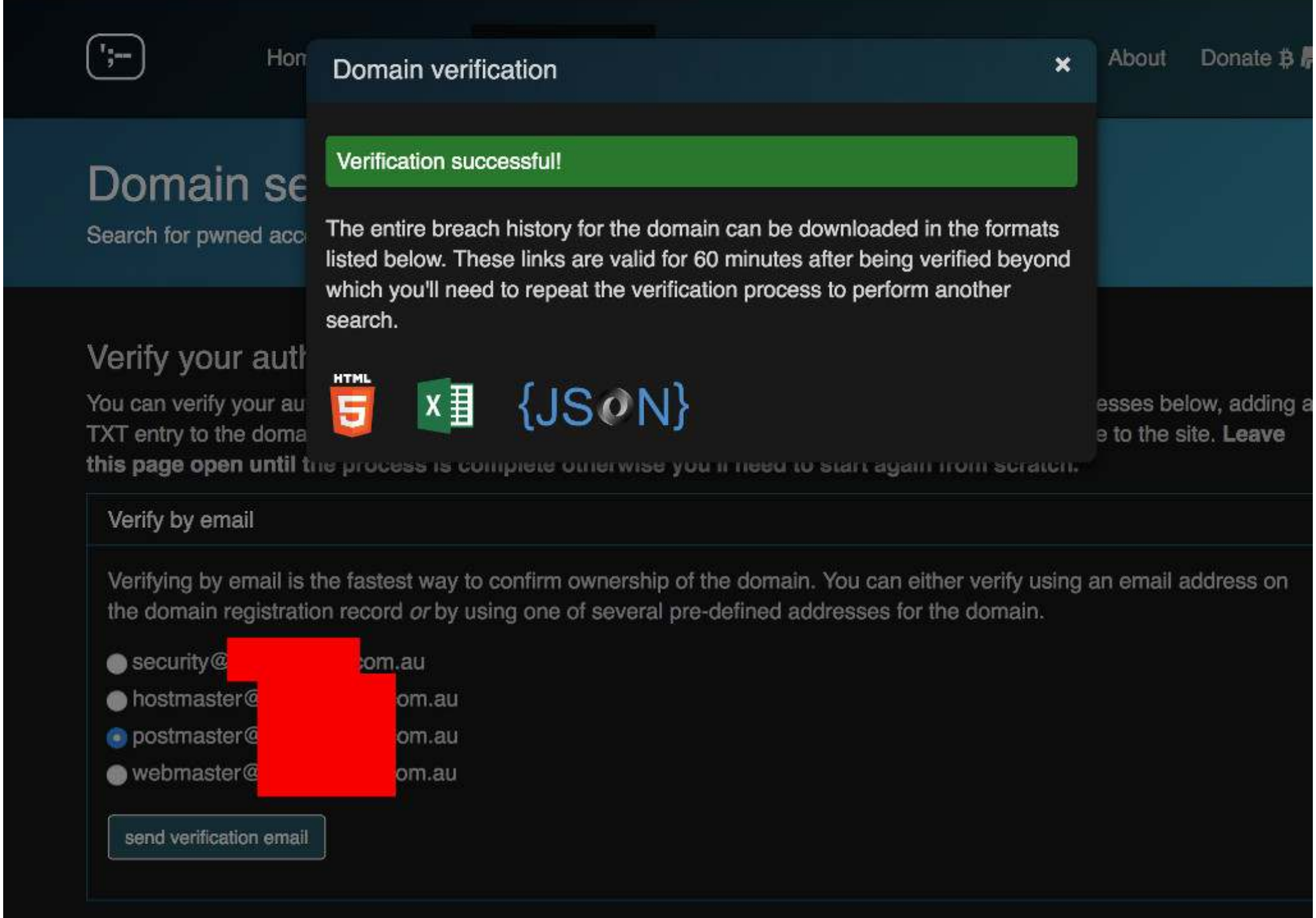

Have I Been Pwned (Troy
[AU]
https://haveibeenpwned.com
Domain search
Who's been pwned
Passwords
API
About
Donate
';--have i been pwned?
Check if you have an account that has been compromised in a data breach
email address
pwned?
Generate secure, unique passwords for every account
Learn more at 1Password.com
Why 1Password?

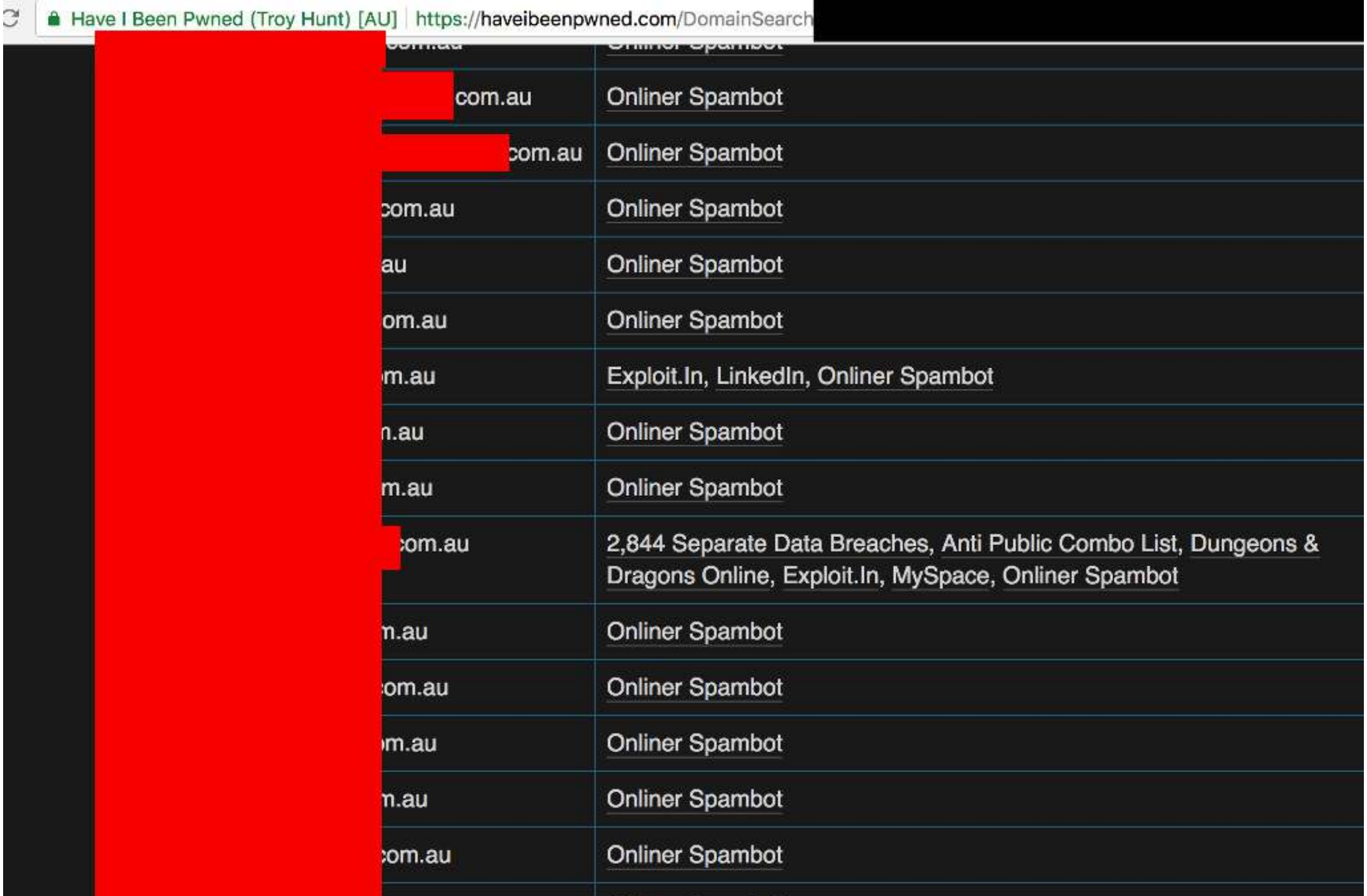
Question 2.

What are the domain verification methods on ‘Havibeenpwned’?

Question 2.

- **Email** – e.g. postmaster@
- **Website –** Meta tag and file upload
- **DNS** – TXT record


Hon
About
Donate
Domain se
Search for pwned acc
Verify your auth
You can verify your au
esses below, adding a
TXT entry to the doma
e to the site. Leave
this page open until the process is complete otherwise you'll need to start again from scratch.
Verify by email
Verifying by email is the fastest way to confirm ownership of the domain. You can either verify using an email address on the domain registration record or by using one of several pre-defined addresses for the domain.
security@
com.au
hostmaster@
om.au
postmaster@
om.au
webmaster@
om.au
send verification email
Domain verification
Verification successful!
The entire breach history for the domain can be downloaded in the formats listed below. These links are valid for 60 minutes after being verified beyond which you'll need to repeat the verification process to perform another search.
HTML
{JSON}


Have I Been Pwned (Troy Hunt) [AU]
https://haveibeenpwned.com/DomainSearch
com.au
Onliner Spambot
com.au
Onliner Spambot
com.au
Onliner Spambot
au
Onliner Spambot
om.au
Onliner Spambot
m.au
Exploit.In, LinkedIn, Onliner Spambot
n.au
Onliner Spambot
m.au
Onliner Spambot
com.au
2,844 Separate Data Breaches, Anti Public Combo List, Dungeons & Dragons Online, Exploit.In, MySpace, Onliner Spambot
m.au
Onliner Spambot
om.au
Onliner Spambot
m.au
Onliner Spambot
m.au
Onliner Spambot
com.au
Onliner Spambot

SpyCloud SOLUTIONS OUR INTEL COMPANY PRICING PARTNERS SIGN IN TRY FOR FREE

PROTECT EMPLOYEES AND CUSTOMERS FROM ACCOUNT TAKEOVER

Stamp out fraud, intellectual property theft, and damage to your brand.

you@email CHECK YOUR EXPOSURE

SpyCloud.com

Take Action Before the Criminals Do

Collect

Match

Prevent

Secure | https://portal.spycloud.com/watchlist/identifiers/view/[redacted]show-tab-corporat...

SpyCloud

[redacted]

Data for [redacted]com.au

Data records matching this email.

Filter | Show Passwords

Email Records (6) | Potential Keylogger Records (0)

Show 10 entries | Column visibility | Search:

Breach Title	SpyCloud Publish Date	Breach Date	Email	Password	Sighting
1M Mixed Combolist	2018-05-08	2018-04-19	[redacted].com.au	[redacted]	1
Combolist of 1.4 Billion Credentials	2017-12-22	2017-12-22	[redacted].com.au	[redacted]	4
Anti-Public Combo list	2017-10-18	2017-10-19	[redacted].com.au	[redacted]	3
Exploit.in	2017-10-09	2017-10-07	[redacted].com.au	[redacted]	2
Dungeons & Dragons Online (February 2013)	2017-03-31	2015-07-03	[redacted].com.au	[redacted]	1
MySpace	2016-10-21	2016-05-27	[redacted].com.au	[redacted]	1

Showing 1 to 6 of 6 entries

1

Casual observation

Lawyers are:

- guilty of using crappy passwords
- tend to reuse them across multiple websites

Loot #4: Password resets

From Dropbox <no-reply@dropbox.com>

Subject **Your Dropbox has stopped syncing**

To [redacted]

Reply | Reply All | Forward | Archive | Junk | Delete | M

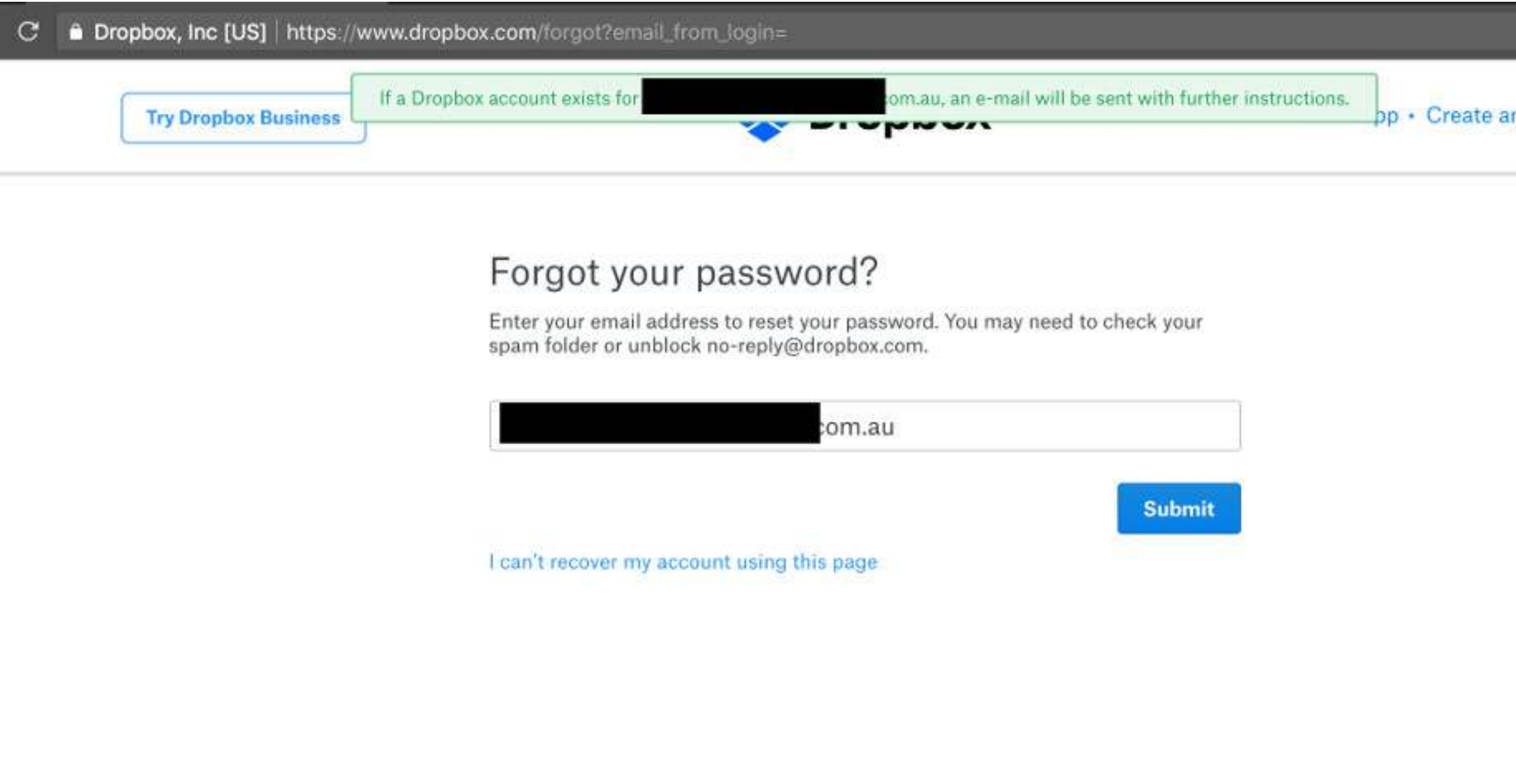
18/7/18,

Hi [redacted]

Your Dropbox is full and is no longer syncing files. New files added to your Dropbox folder won't be accessible on your other devices and won't be backed up online.

Upgrade your Dropbox today and get up to 1 TB (1,000 GB) of space and powerful sharing features.

Upgrade your Dropbox


Dropbox, Inc [US] | https://www.dropbox.com/forgot?email_from_login=
If a Dropbox account exists for [redacted]om.au, an e-mail will be sent with further instructions.
Try Dropbox Business
Dropbox
pp • Create ar
Forgot your password?
Enter your email address to reset your password. You may need to check your spam folder or unblock no-reply@dropbox.com.
[redacted]com.au
Submit
I can't recover my account using this page

From Dropbox <no-reply@dropbox.com>

Subject **Reset your Dropbox password**

To [redacted]

Repl

Hi [redacted]

Someone recently requested a password change for your Dropbox account. If this was you, you can set a new password here:

Reset password

If you don't want to change your password or didn't request this, just ignore and delete this message.

To keep your account secure, please don't forward this email to anyone.

Linked in

[redacted]

Australia | Law Practice

[redacted] connections

Current

Previous

Education

[redacted]

View [redacted]'s full profile.
It's free!

Your colleagues, classmates, and 500 million other professionals are on LinkedIn.

View [redacted] Full Profile

From [redacted] <messages-noreply@linkedin.com>

Subject [redacted]sent you an invitation on LinkedIn

To [redacted]

Reply | Reply All | Forward | Archive

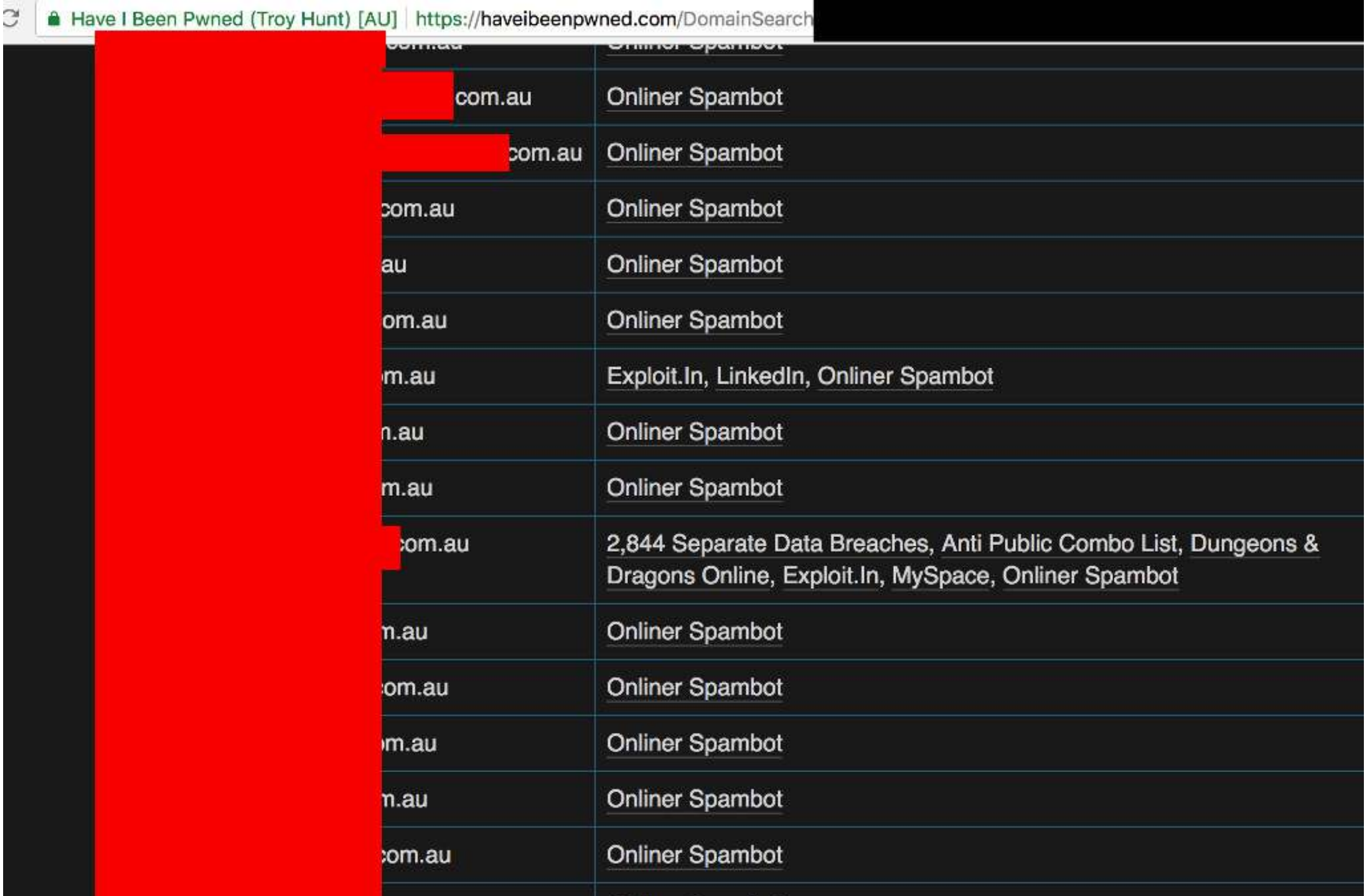
LinkedIn

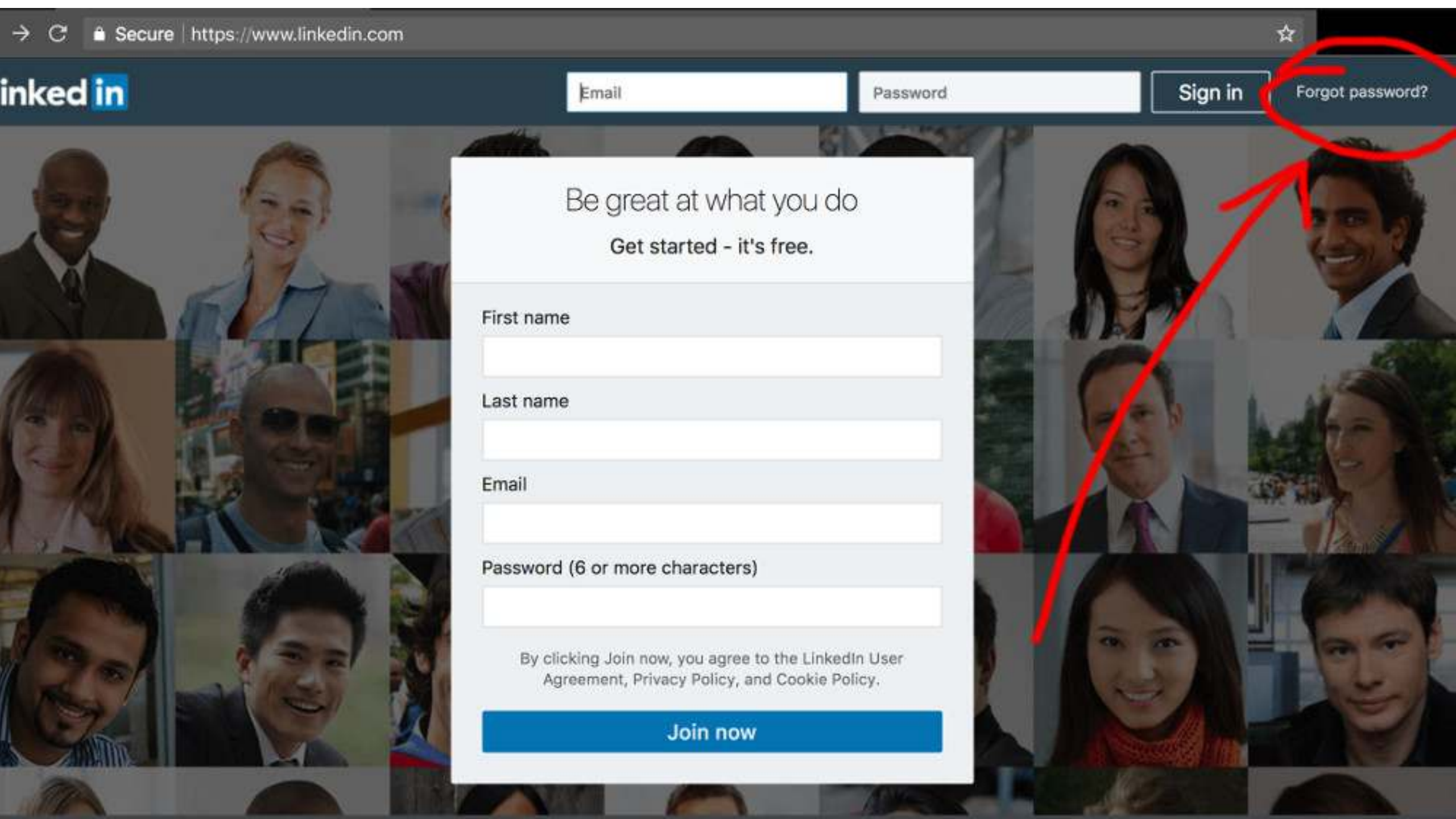
[redacted] wants to add you to their network

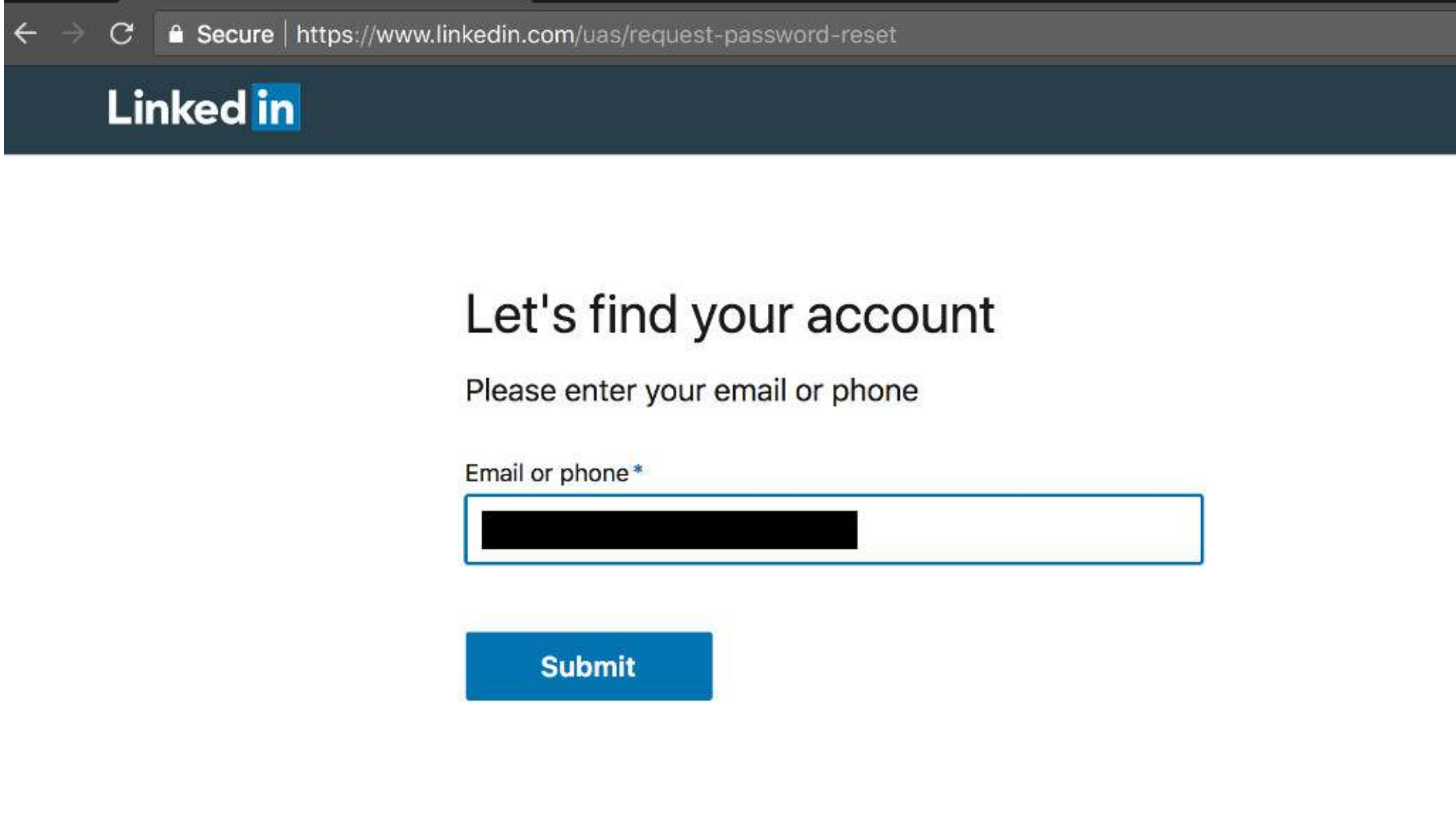
[redacted]
Managing Director at [redacted]
Waikato, New Zealand · [redacted] connections

Accept [redacted]'s invitation

LinkedIn is a social network and online platform for professionals. **Learn More**


Have I Been Pwned (Troy Hunt) [AU]
https://haveibeenpwned.com/DomainSearch
com.au
Onliner Spambot
com.au
Onliner Spambot
com.au
Onliner Spambot
au
Onliner Spambot
om.au
Onliner Spambot
m.au
Exploit.In, LinkedIn, Onliner Spambot
n.au
Onliner Spambot
m.au
Onliner Spambot
com.au
2,844 Separate Data Breaches, Anti Public Combo List, Dungeons & Dragons Online, Exploit.In, MySpace, Onliner Spambot
m.au
Onliner Spambot
om.au
Onliner Spambot
m.au
Onliner Spambot
m.au
Onliner Spambot
com.au
Onliner Spambot


Secure | https://www.linkedin.com
linkedin
Email
Password
Sign in
Forgot password?
Be great at what you do
Get started - it's free.
First name
Last name
Email
Password (6 or more characters)
By clicking Join now, you agree to the LinkedIn User Agreement, Privacy Policy, and Cookie Policy.
Join now


Secure | https://www.linkedin.com/uas/request-password-reset
Linked in
Let's find your account
Please enter your email or phone
Email or phone*
Submit

[redacted]here's the link to reset your password

Message 1 of 31

From LinkedIn <security-noreply@linkedin.com>
To [redacted]
Date Today 12:05

Hi [redacted]

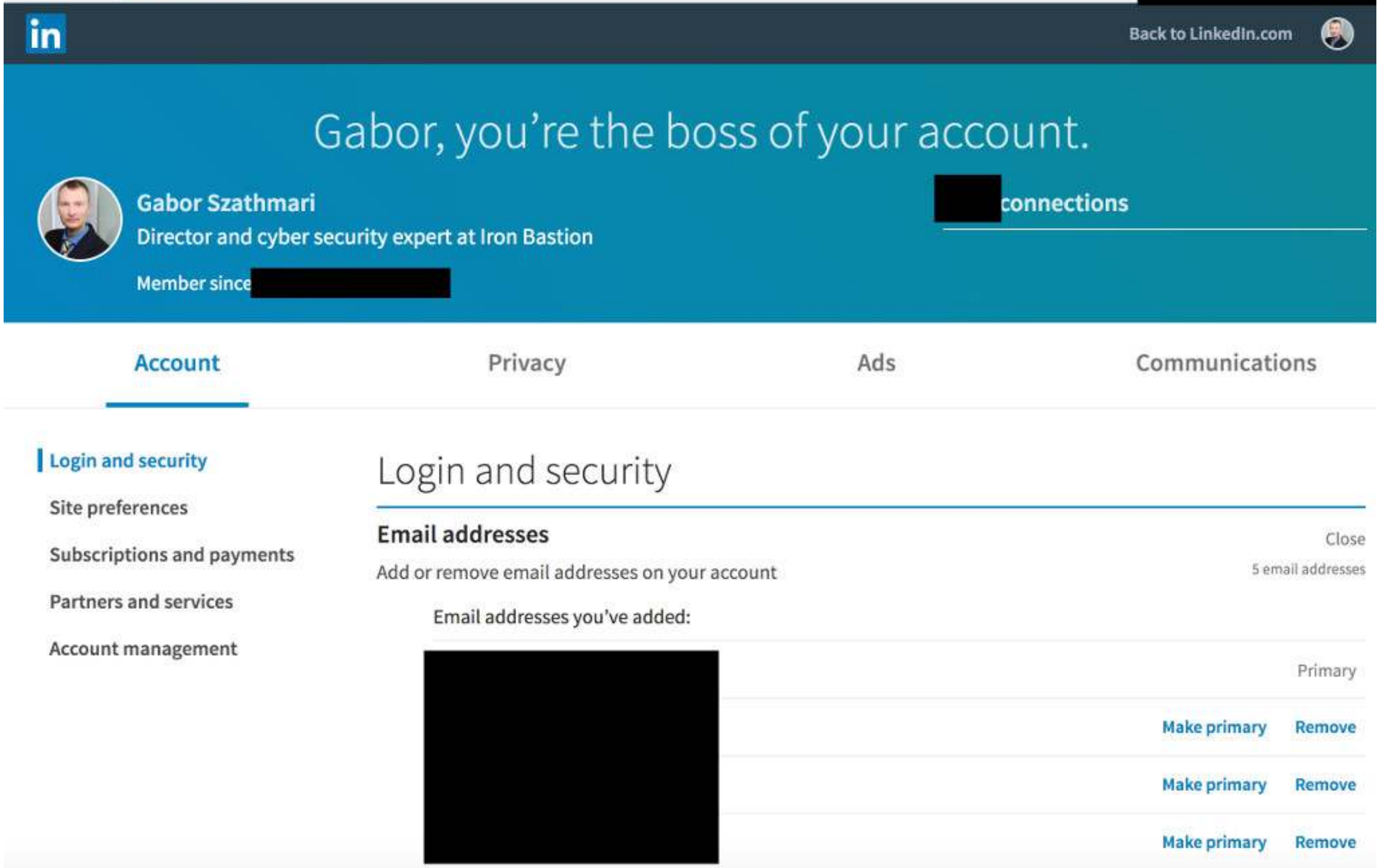
Reset your password, and we'll get you on your way.

To change your LinkedIn password, click here or paste the following link into your browser:

https://www.linkedin.com/e/v2?e=1f63oq-ii9m7r7k-[redacted]

This link will expire in 24 hours, so be sure to use it right away.

Thank you for using LinkedIn!
The LinkedIn Team


Back to LinkedIn.com
Gabor, you're the boss of your account.
Gabor Szathmari
Director and cyber security expert at Iron Bastion
[redacted] connections
Member since [redacted]
Account
Privacy
Ads
Communications
Login and security
Site preferences
Subscriptions and payments
Partners and services
Account management
Login and security
Email addresses
Close
Add or remove email addresses on your account
5 email addresses
Email addresses you've added:
[redacted]
Primary
Make primary
Remove
Make primary
Remove
Make primary
Remove

Secure | https://www.facebook.com[redacted]

[redacted] Gábor Home FBP

[redacted]

Like Follow Recommend ···

[redacted]

See All

Send Message

Send Message

[redacted]

Suggest Edits

Home
About
Reviews
Photos
Posts
Community
Info and Ads

Create a Page

Posts

[redacted] shared a post.

Yesterday at 1:40 PM ·

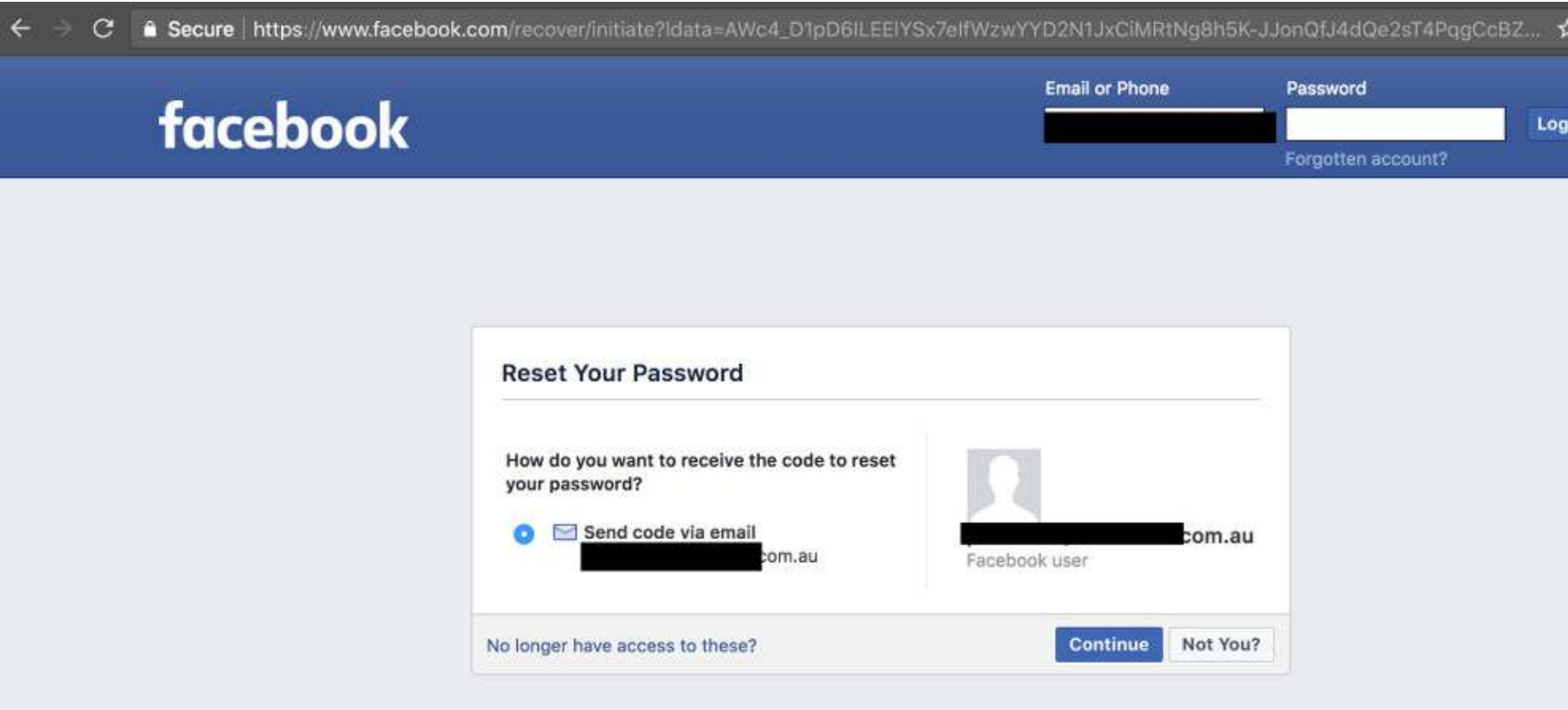
[redacted]

Related Pages

[redacted]

Pages Liked by This Page

[redacted]


Secure | https://www.facebook.com/recover/initiate?ldata=AWc4_D1pD6lLEEIYSx7elfWzwYYD2N1JxCiMRtNg8h5K-JJonQfJ4dQe2sT4PqgCcBZ...
facebook
Email or Phone
Password
Log
Forgotten account?
Reset Your Password
How do you want to receive the code to reset your password?
Send code via email
com.au
com.au
Facebook user
No longer have access to these?
Continue
Not You?

From Facebook <security@facebookmail.com>
Subject **784561 is your Facebook account recovery code**
Reply to noreply <noreply@facebookmail.com>
To [redacted]

Reply | Reply All | Forward | Archive | Junk | Delete | More

18:35

Facebook

Hi [redacted]

We received a request to reset your Facebook password.

Click here to change your password.

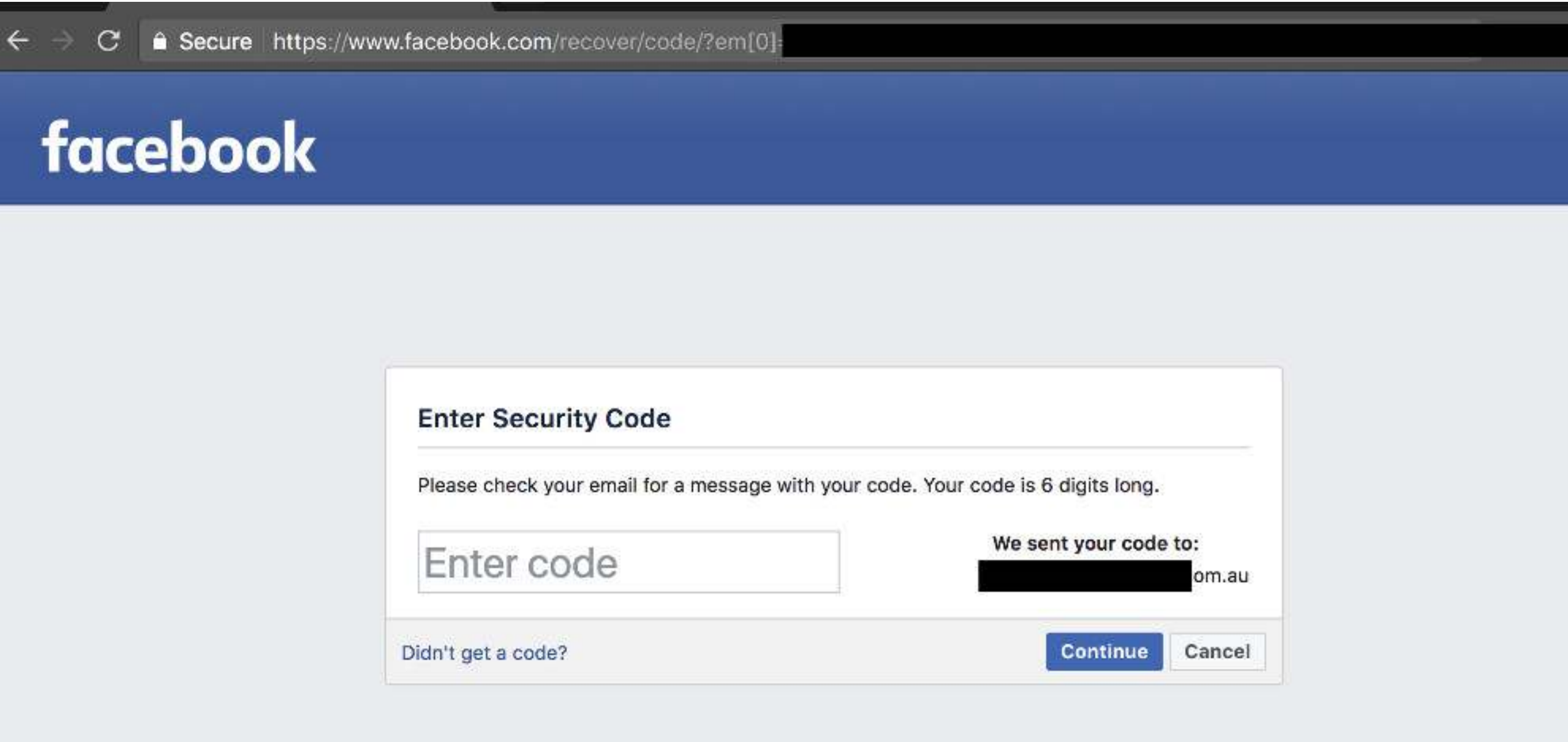
Alternatively, you can enter the following password reset code:

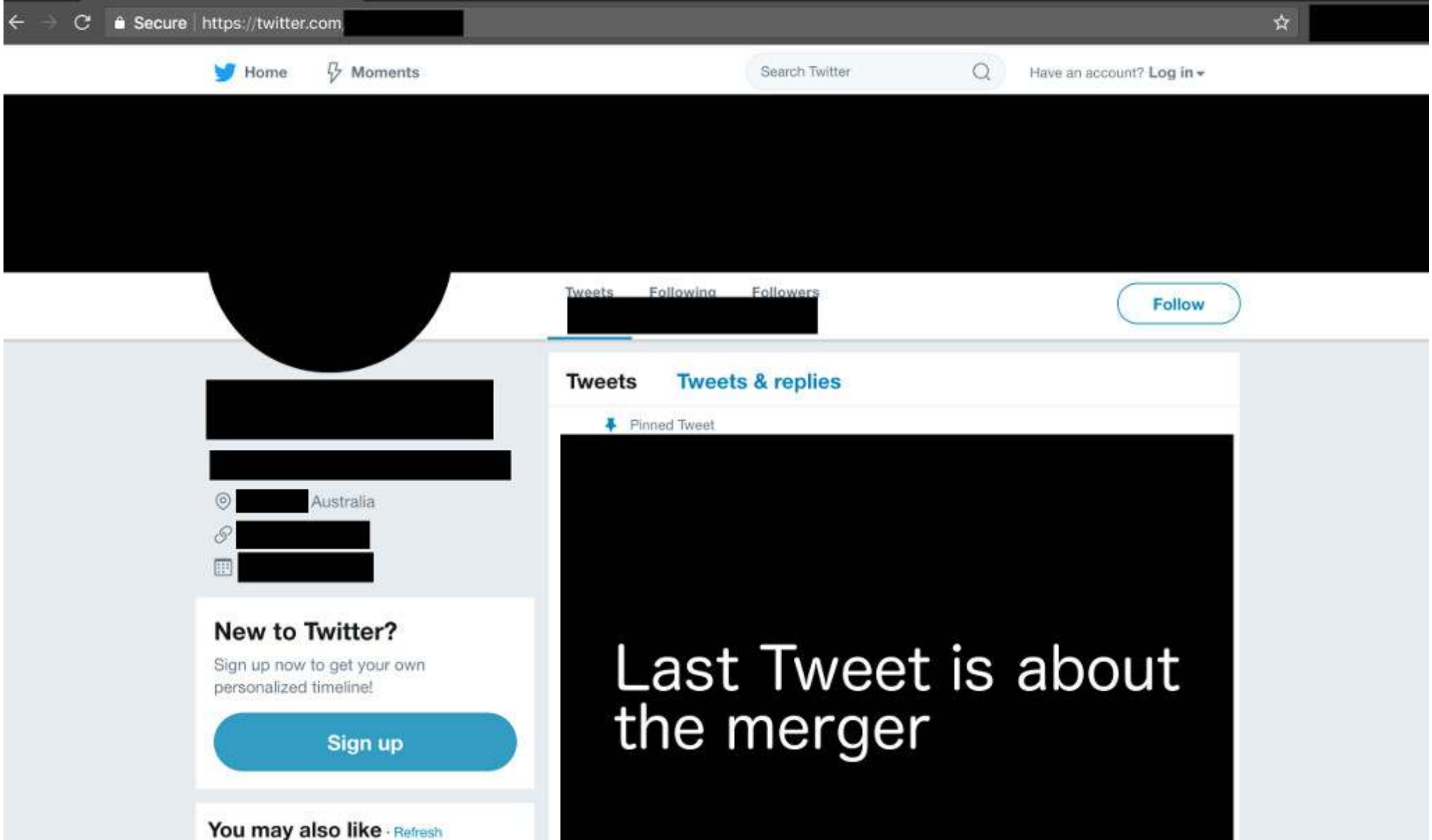
784561

Didn't request this change?
If you didn't request a new password, let us know.

Change Password

This message was sent to [redacted] your request.
Facebook, Inc., Attention: Community Support, 1 Facebook Way, Menlo Park, CA 94025


Secure
https://www.facebook.com/recover/code/?em[0]=
facebook
Enter Security Code
Please check your email for a message with your code. Your code is 6 digits long.
Enter code
We sent your code to:
om.au
Didn't get a code?
Continue
Cancel


Secure https://twitter.com
Home
Moments
Search Twitter
Have an account? Log in
Tweets
Following
Followers
Follow
Australia
Tweets
Tweets & replies
Pinned Tweet
Last Tweet is about the merger
New to Twitter?
Sign up now to get your own personalized timeline!
Sign up
You may also like · Refresh

Twitter, Inc. [US] | https://twitter.com/account/send_password_reset

Password Reset English

How do you want to reset your password?

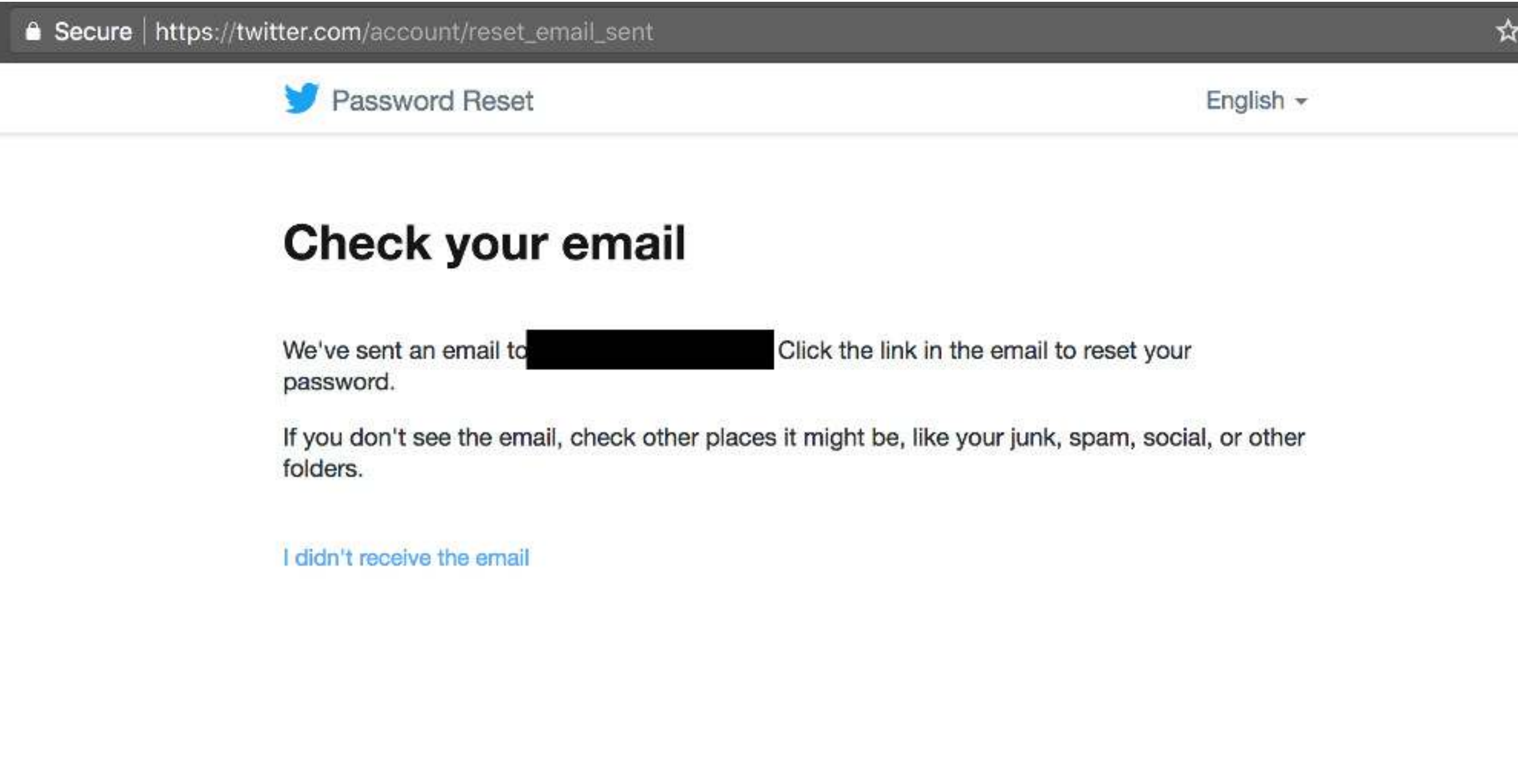
[redacted]

We found the following information associated with your account.

Email a link to [redacted]*******.***.**

Continue

I don't have access to any of these


Secure | https://twitter.com/account/reset_email_sent
Password Reset
English
Check your email
We've sent an email to [redacted] Click the link in the email to reset your password.
If you don't see the email, check other places it might be, like your junk, spam, social, or other folders.
I didn't receive the email

From Twitter <password@twitter.com>

Subject **Password reset request**

To [redacted]

Reply | Reply All | Forward | Archive | Junk | Delete | More

19:03

Reset your password?

If you requested a password reset for [redacted] click the button below. If you didn't make this request, ignore this email.

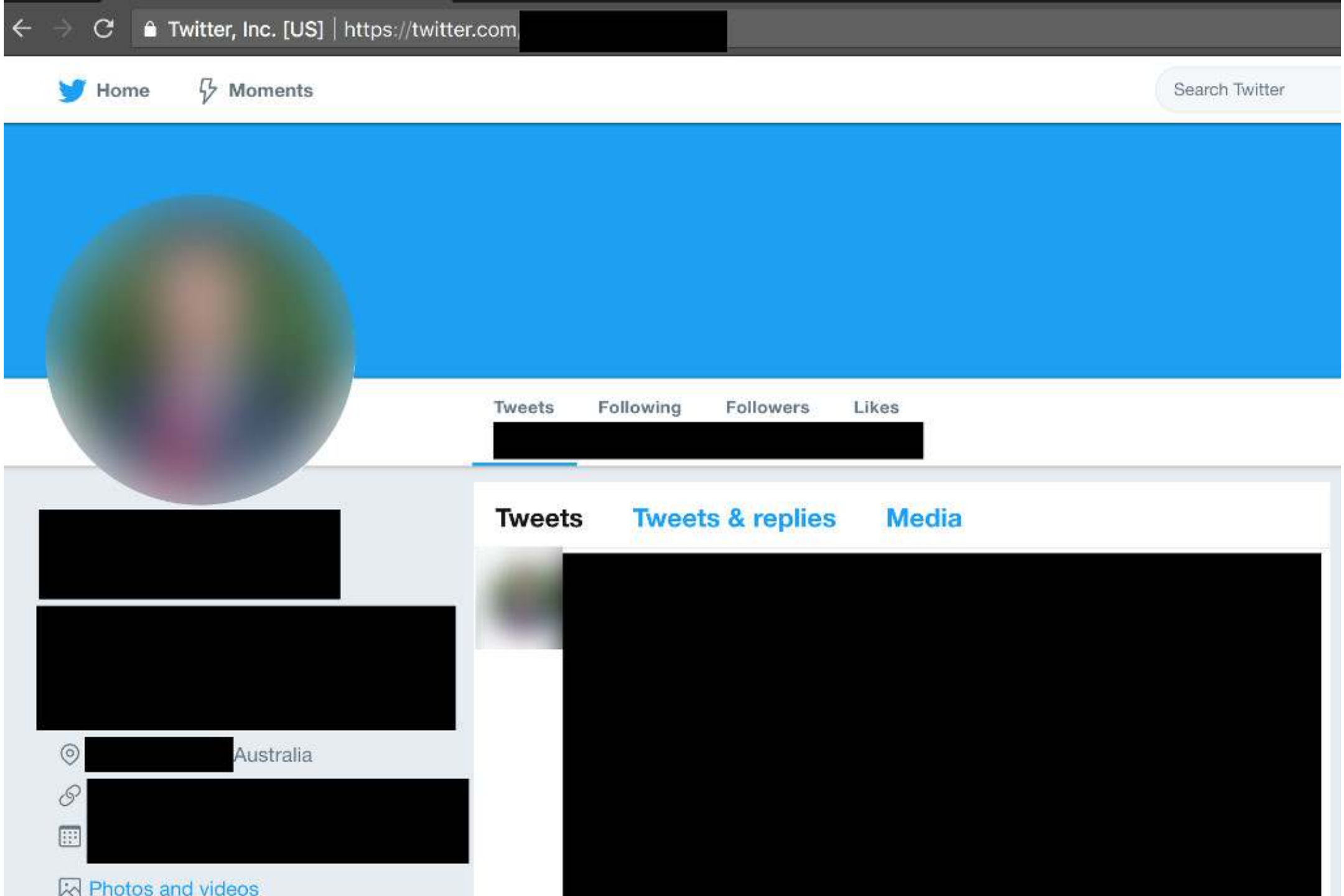
Reset password

Getting a lot of password reset emails?

You can change your account settings to require personal information to reset your password.

How do I know an email is from Twitter?

Links in this email will start with "https://" and contain "twitter.com." Your browser will also display a padlock icon to let you know a site is secure.


Twitter, Inc. [US] | https://twitter.com
Home
Moments
Search Twitter
Tweets
Following
Followers
Likes
Tweets
Tweets & replies
Media
Australia
Photos and videos

Loot #5: Professional-specific portals

Commonwealth Courts Portal

Welcome to the Commonwealth Courts Portal

The Commonwealth Courts Portal is an initiative of the Family Court of Australia, Federal Court of Australia and Federal Circuit Court of Australia. It provides web-based services for clients to access information about cases before the courts.

If you have already registered, please enter your user name and password to login

If you have not registered, you will need to **Register now**

Federal Law Search provides selected information on cases initiated in the Federal Court of Australia and in the federal law jurisdiction of the Federal Circuit Court of Australia.

Family Law eService Obtain Proof of Divorce or Pay Hearing Fees without registering and logging on to the Commonwealth Courts Portal.

News and updates

New users

New users can Register now

Registered users

User name:

Password:

Login

Forgotten user name
Forgotten password

OFFLINE

Secure | https://www.comcourts.gov.au/pacm/access/forgot_password

Family Court of Australia | Federal Court of Australia | Federal Circuit Court of Australia

Commonwealth Courts Portal

Home

Federal Law Search

Forgotten password

If you have previously registered for the Commonwealth Courts Portal and have forgotten your password, enter your user name and email address you would like a new password sent to. The email address must be one registered with your user name.

User name: [redacted]

Email address: [redacted]

Submit

Forgotten user name

Have you changed email address?
If you no longer have access to the email account you used to register with the Commonwealth Courts Portal, please call 1300 352 000.

From noreply@comcourts.gov.au ☆

Reply | Reply All

Subject **Commonwealth Courts Portal - Forgotten password**

To [redacted]

Dear [redacted]

Please use the provided temporary password [redacted] to log on. Once you have logged on, you will b

Regards

The Commonwealth Courts Portal Team
email: support@comcourts.gov.au
www.comcourts.gov.au

Legal Practice Management Software

Explore all the features in LEAP that you need to run an efficient and productive law firm.

Mobile Applications

The LEAP Mobile App for iPhone, iPad and Android devices gives you the freedom to manage your matters from the palm of your hand - wherever you are.

Learn more about Mobile Applications →

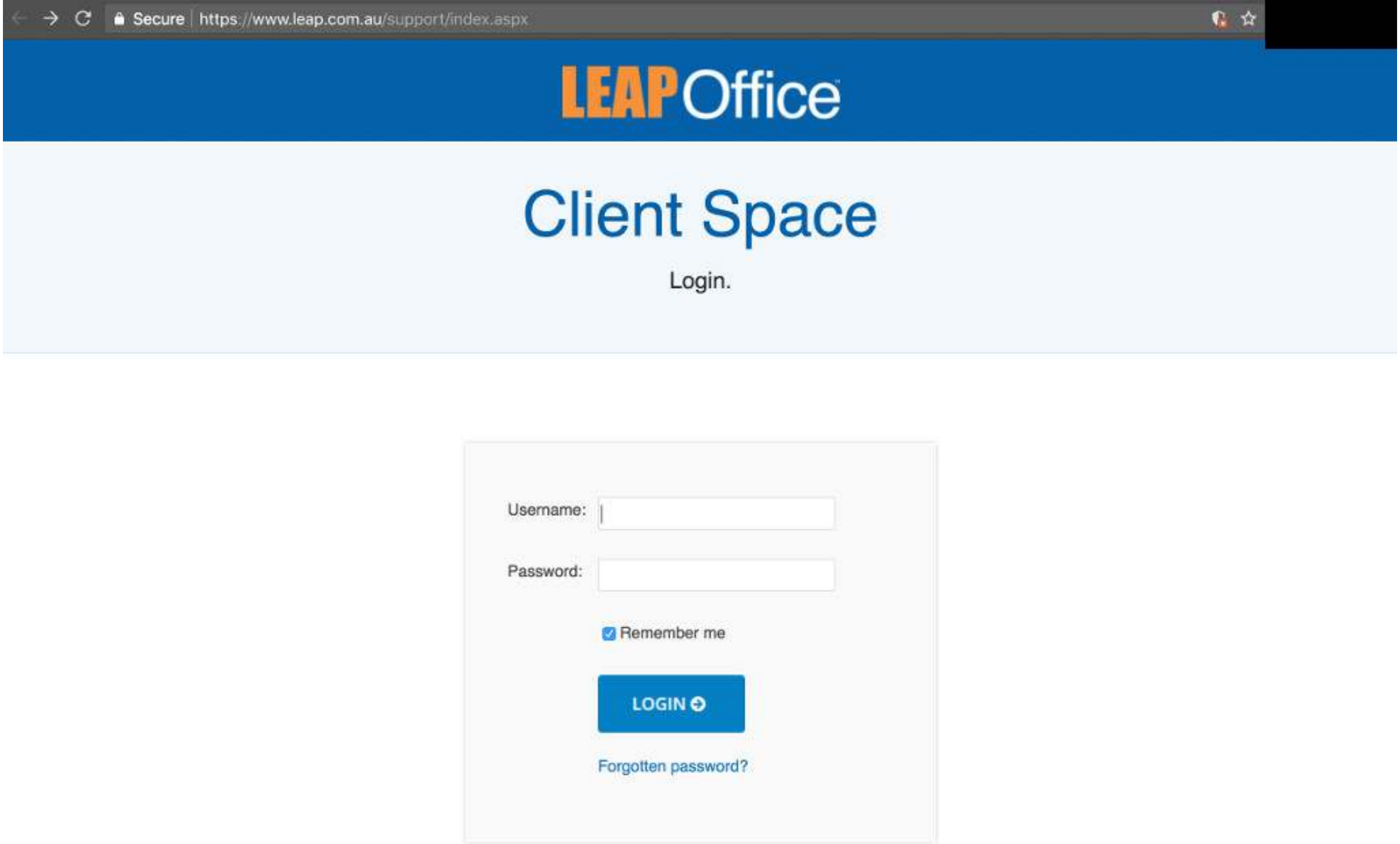
Matter Management

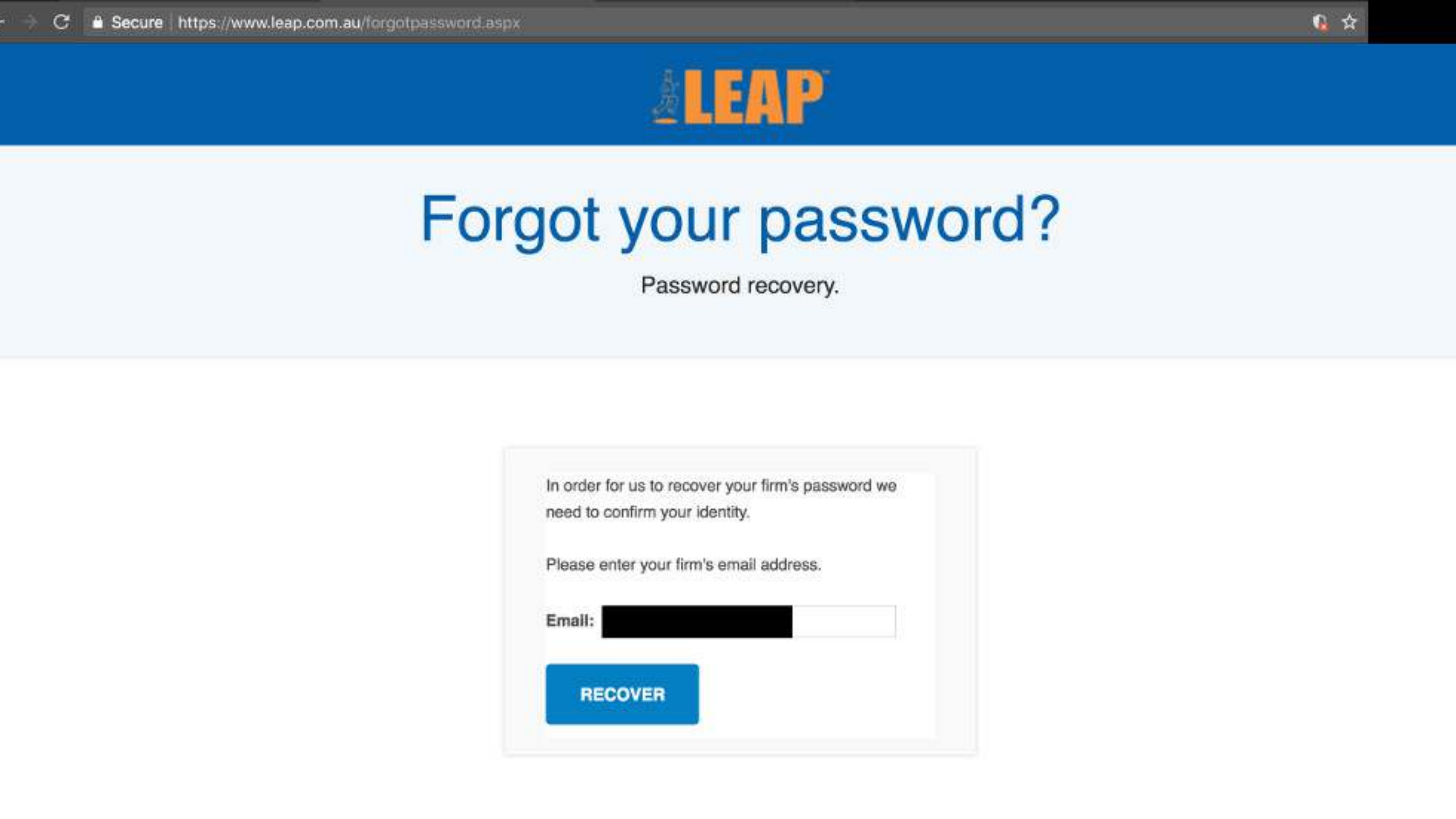
All your matter information is in one place, allowing your staff access to the most up-to-date information and eliminating duplication.

Learn more about Matter Management →

Email Management

Legal Content


Secure | https://www.leap.com.au/support/index.aspx
LEAP Office
Client Space
Login.
Username:
Password:
Remember me
LOGIN
Forgotten password?


Secure
https://www.leap.com.au/forgotpassword.aspx
LEAP
Forgot your password?
Password recovery.
In order for us to recover your firm's password we need to confirm your identity.
Please enter your firm's email address.
Email:
RECOVER

From donotreply@leap.com.au

Subject **Request Account Details for LEAP Legal Software -** [redacted]

To [redacted]

Reply | Reply All | Forward | Archive

NHD Top

Hi,

You are receiving this email from LEAP Legal Software because you requested to recover your password.

Please find below your login details.
Username: [redacted]
Password: [redacted]

You are now ready to login to our website at http://www.leap.com.au. If you experience any problems, please contact us on 1800 007 709.

Thank you,

LEAP Legal Software

NHD Btm

What else we could've accessed?

- NSW Online Registry
- PayPal (accounts@mylawfirm.com.au)
- Google AdWords
- G Suite admin panel
- Office 365 admin portal

Recap

- Sensitive data in emails
- List of email accounts at haveibeenpwned
- Passwords from SpyCloud
- Password reset emails

How to prevent pwnage? (1/2)

- **Keep renewing the domain name indefinitely;**
- Close user accounts that were registered with the business email address
  (e.g. Dropbox, Commonwealth Courts Portal, PayPal);
- Change or remove the business email address from online user accounts (e.g. LinkedIn, Facebook);

How to prevent pwnage? (2/2)

- Unsubscribe from email notifications that usually features sensitive data (Text-to-email services, mobile phone billing notifications);
- Advise your clients to update their address book;
- Enable two-factor authentication where the feature is supported for online services; and
- Use unique and complex passwords.

Red Teams
Blue Teams

Abandoned versus new domains

Better reputation:

- Backlinks/SEO on Google
- Proxy category
- Spam – Not flagged as a newly registered domain

Blue Teams – Protect my organisation

- Phishing against my organisation
- Information leakage (via ‘catch all’ email service)
- Shadow IT takeover (e.g. rogue Dropbox accounts)
- www. or *. → Web traffic / API traffic / iframe/ embedded content hijacking
- Haveibeenpwned, SpyCloud

Red Teams – Security assessments

- Ideal for phishing campaigns
- Gather leaked credentials
- Provides access to 3rd party online services

Question 3.

Can you name three domain reputation services?*

* Used by proxy servers

Question 3.

- Fortinet - http://url.fortinet.net/rate/submit.php
- McAfee - https://www.trustedsource.org/en/feedback/url
- Trend Micro - https://global.sitesafety.trendmicro.com/index.php
- Symantec WebPulse Site Review - https://sitereview.bluecoat.com/
- Barracuda Central - http://www.barracudacentral.org/report/website-category

Tooling

- Ubuntu + Postfix + Dovecot
- Domain registration:
  - Manual
  - API – Above.com
  - Domain backorders
  - ‘Drop catch’ services
    (e.g. www.dropcatch.com, www.drop.com.au)

Summary

- Expired domains are tied to your personal/professional online presence in unexpected ways
- Overlooked attack vector (Red Teams)
- Achilles's Heel of your organisation (Blue Teams)
- ProTip™: Keep your domain names registered

Fun facts

In this research, we:

- Registered six abandoned domain names
- Received approximately 25,000 emails in total
- Won $250,000 from Mark Zuckerberg himself (we are yet to claim the prize)

Questions?

https://blog.gaborszathmari.me/2018/08/22/hacking-law-firms-abandoned-domain-name-attack/

@gszathmari