

Two-Factor Authentication

Laurent Poulain

On the importance of keeping an account secure

- At work, hackers try to get an employee credentials, then move laterally
- At home, most of us have one “master” personal email account
- It can be used to know what bank Website you are using
- It can be used to reset passwords

“I’m using Two-Factor
Authentication (2FA) so I
am secure”

Right?

SIM hijacking can break 2FA

- Hackers convince your cellular carrier to send them a new SIM card
- They can then steal your phone number
- In 2017, several T-Mobile customers were hit after a leak
 - Some customers had their bank account raided
 - Some cryptocurrency users are also targeted

How to prevent SIM hijacking

- Make sure your carrier has some security mechanism
- Use another 2FA mechanism
- Use Google Voice as your recovery number

Many types of second factor authentication

- SMS
- Mobile app providing a code
- Mobile app let you approve the access
- Codes printed on paper
- Physical security key

“OK, I am using a second factor other than SMS. So I’m secure now, right?”

Right?

Demo Time

Yahoo - login

https://login.yahoo.com/config/login?src=fpcbt

Search

Help

YAHOO!

Sign in

laurent.poulain@gmail.com

Next

Stay signed in [Trouble signing in?](#)

Don't have an account? [Sign up](#)

Kali Linux 2018.2 [Running]

Applications Terminal - root@kali: ~ Terminal - root@kali: ~ Terminal - root@kali: ~

Terminal - root@kali: ~

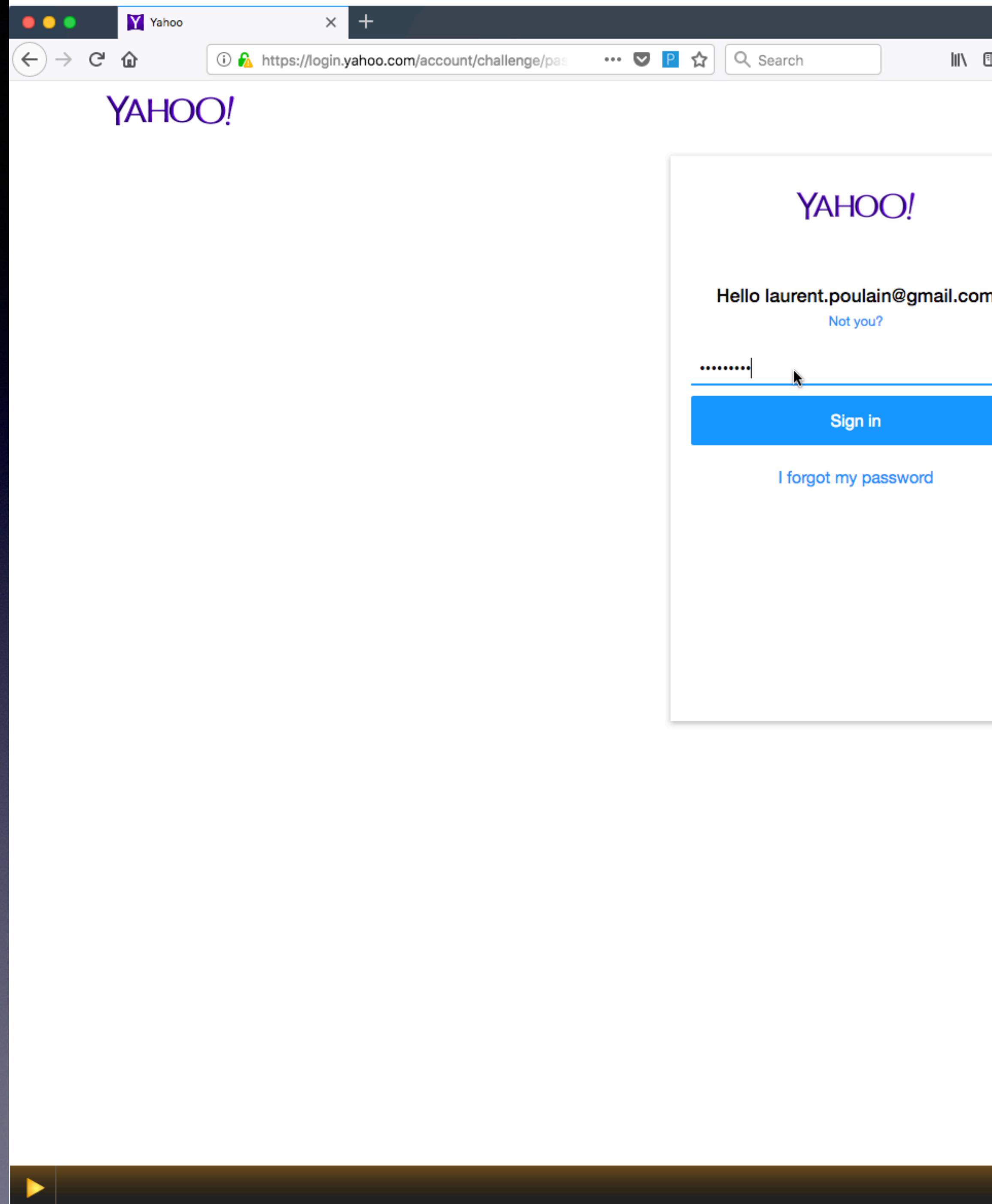
File Edit View Terminal Tabs Help

Flows

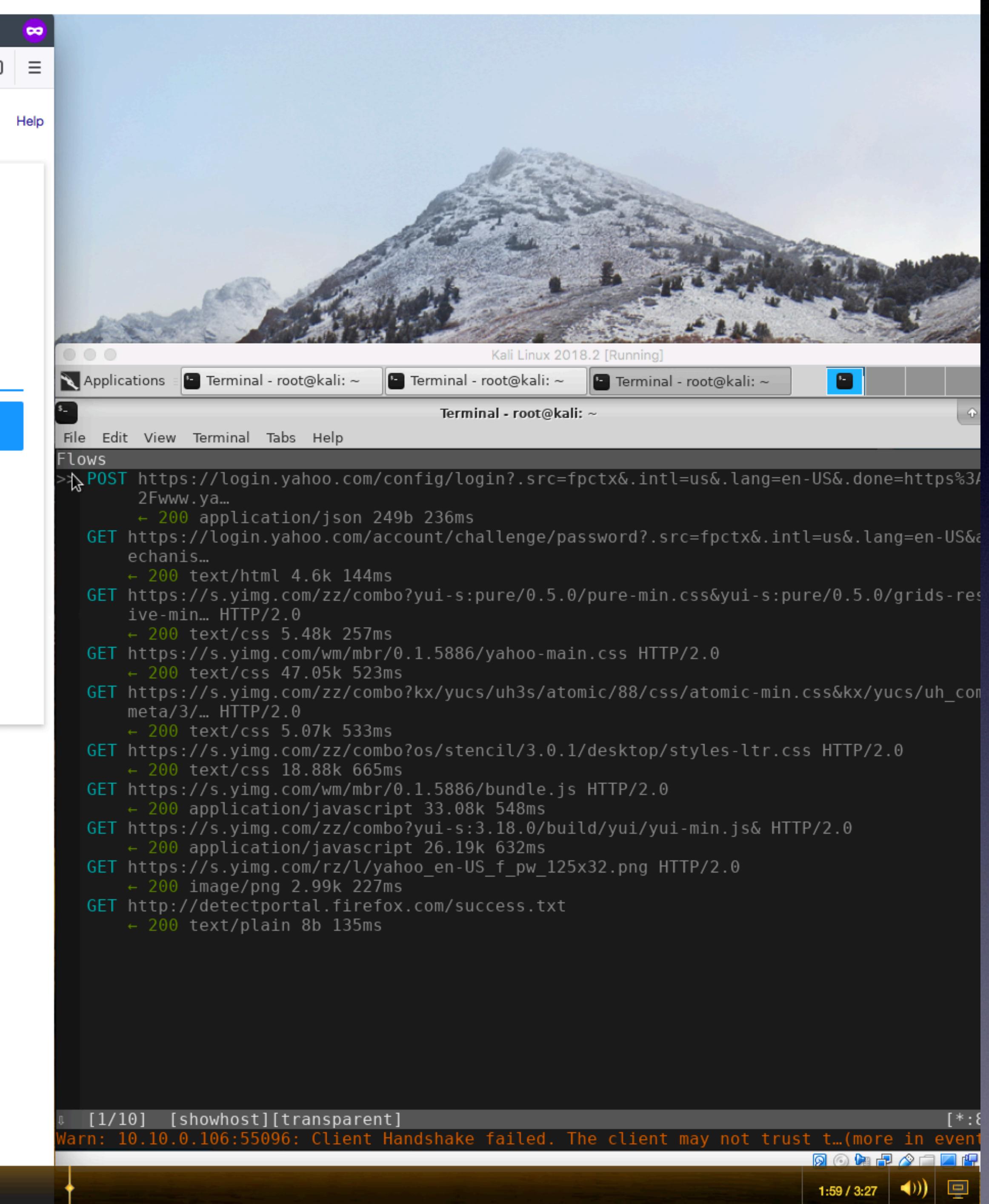
```
[0/0] [showhost][transparent]
Warn: 10.10.0.106:55068: Client Handshake failed. The client may not trust t...(more in event)
```

1:54 / 3:27

Terms (Updated) | Privacy (Updated)



A screenshot of a web browser window showing a Yahoo login page. The URL in the address bar is <https://login.yahoo.com/account/challenge/password?src=fpctx&.intl=us&.lang=en-US&.done=https%3A%2Fwww.yahoo.com%2Faccount%2Fchallenge%2Fpassword%3Fsrc%3Dfpctx%26intl%3Dus%26lang%3Den-US%26done%3Dhttps%253A%252Fwww.yahoo.com%252Faccount%252Fchallenge%252Fpassword>. The page displays the Yahoo logo and a greeting message: "Hello laurent.poulain@gmail.com". Below the greeting is a password input field with placeholder dots and a "Sign in" button. A link "I forgot my password" is also present.



Kali Linux 2018.2 [Running]

Applications Terminal - root@kali: ~ Terminal - root@kali: ~ Terminal - root@kali: ~ Terminal - root@kali: ~

Terminal - root@kali: ~

File Edit View Terminal Tabs Help

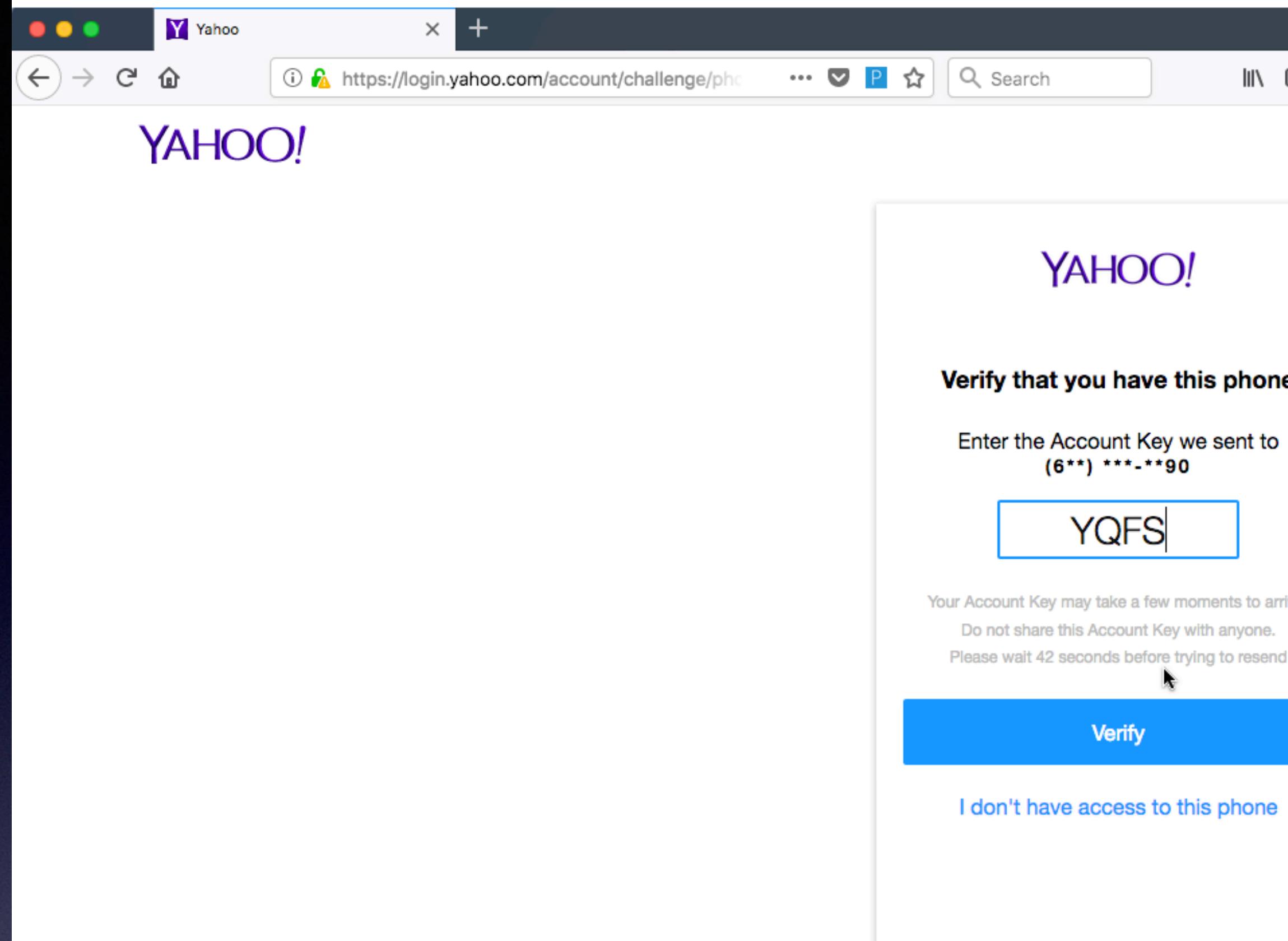
Flows

```
> POST https://login.yahoo.com/config/login?.src=fpctx&.intl=us&.lang=en-US&.done=https%3A%2Fwww.yahoo.com%2Faccount%2Fchallenge%2Fpassword%3Fsrc%3Dfpctx%26intl%3Dus%26lang%3Den-US%26done%3Dhttps%253A%252Fwww.yahoo.com%252Faccount%252Fchallenge%252Fpassword
2Fwww.ya...
← 200 application/json 249b 236ms
GET https://login.yahoo.com/account/challenge/password?.src=fpctx&.intl=us&.lang=en-US&.done=https%3A%2Fwww.yahoo.com%2Faccount%2Fchallenge%2Fpassword%3Fsrc%3Dfpctx%26intl%3Dus%26lang%3Den-US%26done%3Dhttps%253A%252Fwww.yahoo.com%252Faccount%252Fchallenge%252Fpassword
echanis...
← 200 text/html 4.6k 144ms
GET https://s.yimg.com/zz/combo?yui-s:pure/0.5.0/pure-min.css&yui-s:pure/0.5.0/grids-resive-min... HTTP/2.0
← 200 text/css 5.48k 257ms
GET https://s.yimg.com/wm/mbr/0.1.5886/yahoo-main.css HTTP/2.0
← 200 text/css 47.05k 523ms
GET https://s.yimg.com/zz/combo?kx/yucs/uh3s/atomic/88/css/atomic-min.css&kx/yucs/uh_commeta/3/... HTTP/2.0
← 200 text/css 5.07k 533ms
GET https://s.yimg.com/zz/combo?os/stencil/3.0.1/desktop/styles-ltr.css HTTP/2.0
← 200 text/css 18.88k 665ms
GET https://s.yimg.com/wm/mbr/0.1.5886/bundle.js HTTP/2.0
← 200 application/javascript 33.08k 548ms
GET https://s.yimg.com/zz/combo?yui-s:3.18.0/build/yui/yui-min.js& HTTP/2.0
← 200 application/javascript 26.19k 632ms
GET https://s.yimg.com/rz/l/yahoo_en-US_f_pw_125x32.png HTTP/2.0
← 200 image/png 2.99k 227ms
GET http://detectportal.firefox.com/success.txt
← 200 text/plain 8b 135ms
```

[1/10] [showhost][transparent]

Warn: 10.10.0.106:55096: Client Handshake failed. The client may not trust t...(more in event)

1:59 / 3:27



YAHOO!

YAHOO!

Verify that you have this phone

Enter the Account Key we sent to
(6**) ***-**90

YQFS

Your Account Key may take a few moments to arrive.
Do not share this Account Key with anyone.
Please wait 42 seconds before trying to resend

Verify

I don't have access to this phone

Kali Linux 2018.2 [Running]

Applications Terminal - root@kali: ~ Terminal - root@kali: ~ Terminal - root@kali: ~

Terminal - root@kali: ~

File Edit View Terminal Tabs Help

Flows

```
> POST https://login.yahoo.com/config/login?.src=fpctx&.intl=us&.lang=en-US&.done=https%3A%2Fwww.ya... ← 200 application/json 249b 236ms
GET https://login.yahoo.com/account/challenge/password?.src=fpctx&.intl=us&.lang=en-US&mechanis... ← 200 text/html 4.6k 144ms
GET https://s.yimg.com/zz/combo?yui-s:pure/0.5.0/pure-min.css&yui-s:pure/0.5.0/grids-resive-min... HTTP/2.0 ← 200 text/css 5.48k 257ms
GET https://s.yimg.com/wm/mbr/0.1.5886/yahoo-main.css HTTP/2.0 ← 200 text/css 47.05k 523ms
GET https://s.yimg.com/zz/combo?kx/yucs/uh3s/atomic/88/css/atomic-min.css&kx/yucs/uh_commeta/3/... HTTP/2.0 ← 200 text/css 5.07k 533ms
GET https://s.yimg.com/zz/combo?os/stencil/3.0.1/desktop/styles-ltr.css HTTP/2.0 ← 200 text/css 18.88k 665ms
GET https://s.yimg.com/wm/mbr/0.1.5886/bundle.js HTTP/2.0 ← 200 application/javascript 33.08k 548ms
GET https://s.yimg.com/zz/combo?yui-s:3.18.0/build/yui/yui-min.js& HTTP/2.0 ← 200 application/javascript 26.19k 632ms
GET https://s.yimg.com/rz/l/yahoo_en-US_f_pw_125x32.png HTTP/2.0 ← 200 image/png 2.99k 227ms
GET http://detectportal.firefox.com/success.txt ← 200 text/plain 8b 135ms
GET https://s.yimg.com/wm/modern/images/fuji-spinner-1.0.1.svg HTTP/2.0 ← 200 image/svg+xml 614b 169ms
POST https://login.yahoo.com/account/challenge/password?.src=fpctx&.intl=us&.lang=en-US&mechanis... ← 302 text/html 522b 312ms
GET https://login.yahoo.com/account/challenge/challenge-selector?.src=fpctx&.intl=us&.lang=en-US&au... ← 200 text/html 4.73k 193ms
GET http://detectportal.firefox.com/success.txt
```

[*:80] [showhost][transparent]

Warn: 10.10.0.106:55180: Client Handshake failed. The client may not trust t...(more in event log)

2:26 / 3:27

Yahoo

https://www.yahoo.com/?guccounter=1

Home Mail Flickr Tumblr Entertainment Lifestyle Mobile View More

YAHOO!

Mail News Finance Sports Politics Entertainment

Royal Wedding Watch Prince Harry and Meghan Markle get married LIVE on Saturday

Yahoo will stream the historic event from 5 a.m. to 10 a.m. ET

Expert warns about threat of killer robots

A New School professor warns about the potential future threat of a computer that could New weapons of mass destruction? »

[Make Yahoo your homepage](#)

Trending Now

1. Real Madrid	6. Car Donation
2. Leonardo DiCaprio	7. Jane Fonda
3. Ayissha Morgan	8. Car Insurance
4. Tom Welling	9. Houston Astros Ti...
5. Hilary Duff	10. Lorena Hernandez

When Harry met Meghan: From blind date to wedding Kim K. ad sparks social media uproar Pliskova fakes handshake, attacks chair after loss Why Americans are rushing to buy houses Alec Baldwin, 60, is a dad again

U.S. Delish

That Scumbag Lawyer's Racist Rant Is Costing Him

Angry lawyer who went on a racist rant apparently called the police when confronted by reporters Business Insider

Racist lawyer defended Trump's Mexican 'rapists' comments New York Post

Sponsored by TotalAV

Performing a TLS handshake to beap-bc.yahoo.com...

Kali Linux 2018.2 [Running]

Applications Terminal - root@kali: ~ Terminal - root@kali: ~ Terminal - root@kali: ~

Terminal - root@kali: ~

File Edit View Terminal Tabs Help

Flows

```
> POST https://login.yahoo.com/config/login?.src=fpctx&.intl=us&.lang=en-US&.done=https%3A%2Fwww.ya... 200 application/json 249b 236ms
< 200 text/html 4.6k 144ms
GET https://login.yahoo.com/account/challenge/password?.src=fpctx&.intl=us&.lang=en-US&mechanis... 200 text/css 5.48k 257ms
GET https://s.yimg.com/zz/combo?yui-s:pure/0.5.0/pure-min.css&yui-s:pure/0.5.0/grids-resive-min... HTTP/2.0 200 text/css 5.48k 257ms
GET https://s.yimg.com/wm/mbr/0.1.5886/yahoo-main.css HTTP/2.0 200 text/css 47.05k 523ms
GET https://s.yimg.com/zz/combo?kx/yucs/uh3s/atomic/88/css/atomic-min.css&kx/yucs/uh_com... meta/3... HTTP/2.0 200 text/css 5.07k 533ms
GET https://s.yimg.com/zz/combo?os/stencil/3.0.1/desktop/styles-ltr.css HTTP/2.0 200 text/css 18.88k 665ms
GET https://s.yimg.com/wm/mbr/0.1.5886/bundle.js HTTP/2.0 200 application/javascript 33.08k 548ms
GET https://s.yimg.com/zz/combo?yui-s:3.18.0/build/yui/yui-min.js& 200 application/javascript 26.19k 632ms
GET https://s.yimg.com/rz/l/yahoo_en-US_f_pw_125x32.png HTTP/2.0 200 image/png 2.99k 227ms
GET http://detectportal.firefox.com/success.txt 200 text/plain 8b 135ms
GET https://s.yimg.com/wm/modern/images/fuji-spinner-1.0.1.svg HTTP/2.0 200 image/svg+xml 614b 169ms
POST https://login.yahoo.com/account/challenge/password?.src=fpctx&.intl=us&.lang=en-US&mechanis... 302 text/html 522b 312ms
GET https://login.yahoo.com/account/challenge/challenge-selector?.src=fpctx&.intl=us&.lang=en-US&au... 200 text/html 4.73k 193ms
GET http://detectportal.firefox.com/success.txt 200 text/plain 8b 135ms
[*:8] [1/109] [showhost][transparent]
Warn: 10.10.0.106:55269: Client Handshake failed. The client may not trust t...(more in event log)
```

2:41 / 3:27

Yahoo

https://www.yahoo.com/?guccounter=1

Home Mail Flickr Tumblr Entertainment Lifestyle Mobile View More Make Yahoo Your Homepage »

YAHOO! Search

Laurent Mail

Mail News Finance Sports Politics Entertainment Lifestyle More... Close Ad

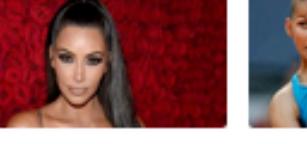
Royal Wedding Watch Prince Harry and Meghan Markle get married LIVE on Saturday

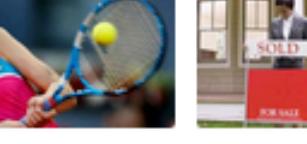
Yahoo will stream the historic event from 5 a.m. to 10 a.m. ET


Expert warns about threat of killer robots
A New School professor warns about the potential future threat of a computer that could
New weapons of mass destruction? »
553 people reacting




When Harry met Meghan: From blind date to wedding


Kim K. ad sparks social media uproar


Pliskova fakes handshake, attacks chair after loss


Why Americans are rushing to buy houses


Alec Baldwin, 60, is a dad again

Trending Now

- 1. Real Madrid
- 2. Leonardo Dicaprio
- 3. Ayissha Morgan
- 4. Tom Welling
- 5. Hilary Duff
- 6. Car Donation
- 7. Jane Fonda
- 8. Car Insurance
- 9. Houston Astros Ti...
- 10. Lorena Hernandez

Make Yahoo your homepage

U.S. Delish
That Scumbag Lawyer's Racist Rant Is Costing Him
Angry lawyer who went on a racist rant apparently called the police when confronted by reporters Business Insider
Racist lawyer defended Trump's Mexican 'rapists' comments New York Post

1973

Sponsored by TotalAV

Kali Linux 2018.2 [Running]

Applications Terminal - root@kali: ~ Terminal - root@kali: ~ Terminal - root@kali: ~

Terminal - root@kali: ~

File Edit View Terminal Tabs Help

Flow Details

2018-05-17 23:05:42 POST https://login.yahoo.com/config/login?.src=fpctx&.intl=us&.lang=en-<done>=<https%3A%2F%2Fwww.yahoo.com> ← 200 OK application/json 249b 236ms

Request Response Detail

Accept-Encoding: gzip, deflate, br
Referer: https://login.yahoo.com/config/login?.src=fpctx&.intl=us&.lang=en-US&do<done>=<https%3A%2F%2Fwww.yahoo.com>
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 121
Cookie: B=3uqq9v9dfsglb&b=3&s=rt; GUCS=ASRzrWNa; ucs=lnct=1526612712; AS=v=1&s=p4w0MG&d=A5aff947a|gxwtCu_.2cIAxFJMXTEE91ER1UIakhLKIgCwgkjQFPkyVZa4xSN3dEsGMA7TQrrCSf6gYIG.7USEEnwzAl1pF3Y5zqhudS.WitEIIldFs38m0HRBKrcbsPrZ_9Z0aMHYll73_UNL102uxyme0c7n_VN7p5AFmc9oPc2k6LvAUUq0YXMIZMCUCQHM11tnSucrTZjirj3mW3kuuxp8wBLQ7ukXLieGXsx0RrcB4NWIVEIWEcmRjosTyrix0Q.LFT.KrHa6T_kkYS4oX31Uy97ZB80B0HenJ.dn5TAfhvZvPwiYq9PtpsE3sJPr146uN4.qLLSM_AEWxDac3umdJsv0jW0QzNKR_L9iw08gTFLFCScTpJFs4Bk3UP0.qHqzubdc8MQw395rBI18d2zqY4zSinvr1q.7CHCHVNVAR4IG5SE9lgEYZV7xoNCAk131PdyCZKqazoW2pMsPoizY2hMAskGvhJ3TEcPxUi_j_0Nw2tVfznAN.XFKPNH8QgEi4m7yjguGEuBoIs00HiaJSf2st3735AXlBaDubz.BLTyMBeL5CNsP59DE8Z3wDID76UT068hIomszpZZ7XLt3mmSKVuve_omg7EToEfEcTrhwWhEYXeRa a7LYg6Rk0k364DQJCmeD0R2KoRvCI0y5eQKH83XB6bTzepnjazeZ8g8HJEj7Bs1aAfYtYWyYydrY1quwX1F9nky04caPzYjqpYSbkiBw96s2lZhveMrHJ0Tp7JJ4kEk94WtDQ9.Qx_tFnAO.kkx3RBRWGKfGgioGX8UpUMViXfuAyGzaReI4Li8d1DISLJn0JYRisWZJ2xzG7YqrragJvlgnij4nD_bnJCA.znvTBxnao2H8vMr0j.787Pn61ymLaQJB5Zs4Pv3~A

Connection: keep-alive

URLEncoded form

crumb: CI2PBZmTLy.
acrumb: puG4w0MG
sessionIndex: 00--
username: laurent_poulain@gmail.com
passwd:
signin: Next
persistent: y

↓ [1/147] [showhost][transparent]
Warn: 10.10.0.106:55310: Client Handshake failed. The client may not trust t...(more in event)

Yahoo

https://www.yahoo.com/?guccounter=1

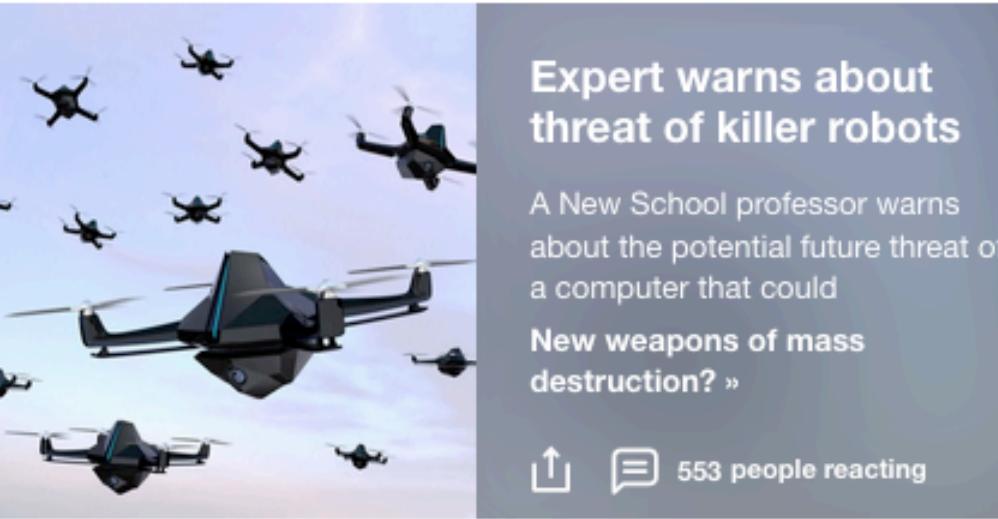
Home Mail Flickr Tumblr Entertainment Lifestyle Mobile View More Make Yahoo Your Homepage »

YAHOO! Search

Laurent Mail

Mail News Finance Sports Politics Entertainment Lifestyle More...

Royal Wedding Watch Prince Harry and Meghan Markle get married LIVE on Saturday
Yahoo will stream the historic event from 5 a.m. to 10 a.m. ET

Expert warns about threat of killer robots
A New School professor warns about the potential future threat of a computer that could
New weapons of mass destruction? »
553 people reacting

Trending Now

- 1. Real Madrid
- 2. Leonardo DiCaprio
- 3. Ayissha Morgan
- 4. Tom Welling
- 5. Hilary Duff
- 6. Car Donation
- 7. Jane Fonda
- 8. Car Insurance
- 9. Houston Astros Ti...
- 10. Lorena Hernandez

When Harry met Meghan: From blind date to wedding **Kim K.** ad sparks social media uproar **Pliskova** fakes handshake, attacks chair after loss **Why Americans are rushing to buy houses** **Alec Baldwin**, 60, is a dad again

U.S. Delish **That Scumbag Lawyer's Racist Rant Is Costing Him**
Angry lawyer who went on a racist rant apparently called the police when confronted by reporters Business Insider
Racist lawyer defended Trump's Mexican 'rapists' comments New York Post

Sponsored by TotalAV

Close Ad X

Kali Linux 2018.2 [Running]

Applications Terminal - root@kali: ~ Terminal - root@kali: ~ Terminal - root@kali: ~

Terminal - root@kali: ~

File Edit View Terminal Tabs Help

Flow Details

2018-05-17 23:05:50 POST https://login.yahoo.com/account/challenge/password?.src=fpxct&.int=.lang=en-US&authMechanis... ← 302 Found text/html 522b 312ms

Request

Tfrt39MTI810Sa50HBmTlJu_G3xEWAY4jkHB9YKwxcHczyRCsDPW_ttM8IJd4t/0RiVQKXWvKszB.Czv9k7WBB87MUDBz6E_FfTK79beT9aRGIIiEnW3btluJ09p0>kEqRM8pfjcz.e.x2pNPN7fDU.LZGKzq5ebykcijs0l_XIVCw1bVrPqLgMT1mBCB0cS5M7vJT6ZpwxeJc2SqzpVpDnYBHS1jVY5LkiUcnf4yRv3G8kKB3Zv_Eklyk8VC TW0XfqsiyQWAtFCaVmvh4q4BLxGz4mXba6o1bG3.fbMDpkPG_5QoaZ5u4nChg60Rq_kfgwv33oAdXh9qS.RWXjJYzjJ.3VVE4hW1CGJF6l6pQBrmoJTGJ_Asy5mKN1sa7eyaa40yKGr854Yyd0hJSleeyWQPL6x0nQ.egsbJdsRKuhHYtIxBoh0m0JWLIE3T5knM0jkKX3DWrvl5gr49rqEFVVPFJtk0BLKGMLNYslc0K7gQW8RB5GmaNjx>aonjvTnP.60ZcX0anNN5dgLT.ZwbAB5r9JDDB6_miIQHt6.Eog0_M06oblujfFGJY2PPgPFIIqvk2fdabcro72B2xgoJ..5Bo034PdCspfVRrUREZ4jpB1eRg_7o4SaM3dPxyoNB062Qqr7ePTQ43VlgA50uyybA0vw--~A keep-alive 1

Connection: Upgrade-Insecure-Requests: 1

URLEncoded form

browser-fp-data: {"language": "en-US", "color_depth": 24, "resolution": {"w": 1920, "h": 1200}, "available_resolution": {"w": 1920, "h": 1178}, "timezone_offset": 240, "session_storage": 1, "local_storage": 1, "indexed_db": 1, "cpu_class": "unknown", "navigator_platform": "MacIntel", "do_not_track": "unspecified", "canvas": "canvas winding:yes~canvas", "webgl": 1, "adblock": 0, "has_lied_languages": 0, "has_lied_resolution": 0, "has_lied_os": 0, "has_lied_browser": 0, "touch_support": {"points": 0, "event": 0, "size": 0}, "plugins": {"count": 0, "hash": "24700f9f1986800ab4fcc880530dd0ed"}, "fonts": {"count": 27, "hash": "d52a1516cfb5f1c2d8a427c14bc3645f"}, "ts": {"serve": 1526612743117, "render": 1526612744608}} crumb: WKwP2IePL6J acrumb: puG4w0MG sessionIndex: QQ-- displayName: laurent.poulain@gmail.com username: laurent.poulain@gmail.com passwordContext: normal password: itsasecret1 verifyPassword: Sign in ↓ [12/151][showhost][transparent] Warn: 10.10.0.106:55348: Client Handshake failed. The client may not trust the certificate (more in event log)

2:58 / 3:27

Yahoo

https://www.yahoo.com/?guccounter=1

Home Mail Flickr Tumblr Entertainment Lifestyle Mobile View More Make Yahoo Your Homepage »

YAHOO! Search

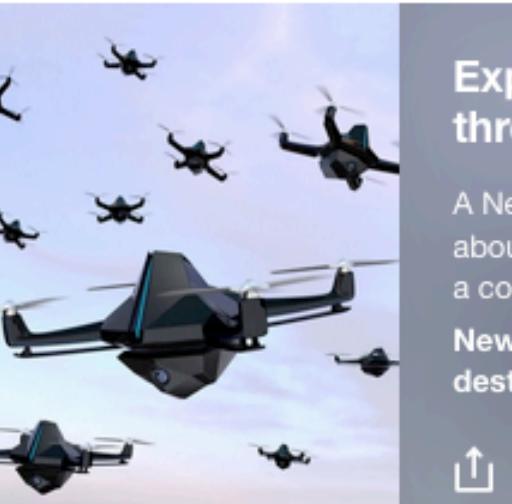
Laurent Mail

Mail News Finance Sports Politics Entertainment Lifestyle More... Close Ad

Royal Wedding Watch Prince Harry and Meghan Markle get married LIVE on Saturday

Yahoo will stream the historic event from 5 a.m. to 10 a.m. ET


Expert warns about threat of killer robots
A New School professor warns about the potential future threat of a computer that could
New weapons of mass destruction? »
553 people reacting



Trending Now

- 1. Real Madrid
- 2. Leonardo DiCaprio
- 3. Ayissha Morgan
- 4. Tom Welling
- 5. Hilary Duff
- 6. Car Donation
- 7. Jane Fonda
- 8. Car Insurance
- 9. Houston Astros Ti...
- 10. Lorena Hernandez

When Harry met Meghan: From blind date to wedding Kim K. ad sparks social media uproar Pliskova fakes handshake, attacks chair after loss Why Americans are rushing to buy houses Alec Baldwin, 60, is a dad again

U.S. Delish That Scumbag Lawyer's Racist Rant Is Costing Him
Angry lawyer who went on a racist rant apparently called the police when confronted by reporters Business Insider
Racist lawyer defended Trump's Mexican 'rapists' comments New York Post

Sponsored by TotalAV

Kali Linux 2018.2 [Running]

Applications Terminal - root@kali: ~ Terminal - root@kali: ~ Terminal - root@kali: ~

Terminal - root@kali: ~

File Edit View Terminal Tabs Help

Flow Details

2018-05-17 23:06:14 POST https://login.yahoo.com/account/challenge/phone-verify?.src=fpctx&l=us&.lang=en-US&authMech... ← 302 Found text/html 292b 358ms

Request Response Detail

LSwMakyKU4BEvoZy72n7qiQlmWemYirg_ManslvzSd92o5hiqvBRvFujLTNTm...
IHOGga2D8M0x5nsyYwGxM5AB75H5VU8417itAeQmqTbx4uGqCKqsrtNYPvg04j...
TRswzEkcESUx.2gkE5AAxqNq02_9fkIETCOHhMGsdbZ2iYev8qMc~A
keep-alive

Connection: Upgrade-Insecure-Requests: 1

URLEncoded form

browser-fp-data: {"language": "en-US", "color_depth": 24, "resolution": {"w": 1920, "h": 1200}, "available_resolution": {"w": 1920, "h": 1178}, "timezone_offset": 240, "session_storage": 1, "localstorage": 1, "indexed_db": 1, "cpu_class": "unknown", "navigator_platform": "MacIntel", "do_not_track": false, "canva...
as_lied_resolution": 0, "has_lied_os": 0, "has_lied_browser": 0, "touch_support": {"points": 0, "events": 0, "start": 0}, "plugins": {"count": 0, "hash": "24700f9f1986800ab4fcc880530dd0ed"}, "fonts": {"count": 7, "hash": "d52a1516cfb5f1c2d8a427c14bc3645f"}, "ts": {"serve": 1526612755089, "render": 1526612755089}}

crumb: WKwP2IePL6J
acrumb: puG4w0MG
sessionIndex: 0
displayName: laurent.poulain@gmail.com
referenceId: fdwBfU.oyTofUnvQsGpvY01SwB16pZvsbcV8mlmMuDZL6hFnkFRcwabJq_QRb65.jv
context: k0kA3znrlcEjw0wMLpM0Fum2gHqSijg16ubgkIasXh7twafZDRhqaAwKGFWIGKpk0ew--
bearer: SECOND_CHALLENGE
codeDigits: sms
obfuscatedPhone: 4
locale: (6**) ***-**90
numberAttemptsRemaining: en-US
45
lastSentTime: 1526612755134
code: YQFS
verifyCode: true
↳ [18/153][showhost][transparent]
Warn: 10.10.0.106:55393: Client Handshake failed. The client may not trust t...(more in event log)

3:10 / 3:27

Yahoo

https://www.yahoo.com/?guccounter=1

Home Mail Flickr Tumblr Entertainment Lifestyle Mobile View More Make Yahoo Your Homepage »

YAHOO! Search

Laurent Mail

Mail News Finance Sports Politics Entertainment Lifestyle More...

Royal Wedding Watch Prince Harry and Meghan Markle get married LIVE on Saturday
Yahoo will stream the historic event from 5 a.m. to 10 a.m. ET


Expert warns about threat of killer robots
A New School professor warns about the potential future threat of a computer that could
New weapons of mass destruction? »
553 people reacting

Trending Now

- 1. Real Madrid
- 2. Leonardo DiCaprio
- 3. Ayissha Morgan
- 4. Tom Welling
- 5. Hilary Duff
- 6. Car Donation
- 7. Jane Fonda
- 8. Car Insurance
- 9. Houston Astros Ti...
- 10. Lorena Hernandez

When Harry met Meghan: From blind date to wedding **Kim K. ad sparks social media uproar** **Pliskova fakes handshake, attacks chair after loss** **Why Americans are rushing to buy houses** **Alec Baldwin, 60, is a dad again**

U.S. Delish
That Scumbag Lawyer's Racist Rant Is Costing Him
Angry lawyer who went on a racist rant apparently called the police when confronted by reporters Business Insider
Racist lawyer defended Trump's Mexican 'rapists' comments New York Post

1973

Sponsored by TotalAV

Kali Linux 2018.2 [Running]

Applications Terminal - root@kali: ~ Terminal - root@kali: ~ Terminal - root@kali: ~

Terminal - root@kali: ~

File Edit View Terminal Tabs Help

Flow Details

2018-05-17 23:06:32 GET https://www.yahoo.com/lib/metro/g/myy/rapidworker_1_2_0.0.5.js HTTP/1.1

+ 200 application/x-javascript [content missing] 18ms

Request Response Detail

:authority: www.yahoo.com
user-agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.13; rv:59.0) Gecko/20100101 Firefox/59.0
accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
accept-language: en-US,en;q=0.5
accept-encoding: gzip, deflate, br
referer: https://www.yahoo.com/
cookie: B=3uqq9v9dfsglb&b=4&d=rB_q2KhpYEL8okIRTsup_A--&s=j7&i=1o5knwrfkPLxEr7IcaGUcS=AQSw0_Nx; flash_enabled=0; ucs=lnct=1526612712; apeaf=td-applet-stre=%7B%22tmp%22%3A%22items%22%2C%22lv%22%3A1526614512352%7D; T=z=mMk/aBmgLB3I1LHzUJvnDMzUwMwYzMjQwNDAxMTM2NE4yNz&a=QAE&sk=DAAJ2Y998V/z8L&ks=EAA2etFdWORl4xioP26E2uQ--~G&k=EAApzLa90WPjo.XnPPIe9QpgA--~I&ku=FAAwnNuMZYkm9DelKbDFWz6NfIJXP_XwF_HPJHvCYy9CpSP3dTa5fXjJSx_PBDXd3r7LKK9U0K8awsX2jsz69hNSmmbc1T0ccV.F6VnhUYxLWJY3nE7tR9r.M85rbfn93ZNIK6v04DAUsGZjcyjMMGXsw9k8750X.HmVuno~~A&d=bnMBewFob28BZwFONFdDVl1RT0dIQ1RaN0tYS01KREM1SUTMRQFzbAFOREkz1FME5UTTNemMyTmpReE16azFNRFE0TVRrLQFhAVFBRQFhYwFBTGxGcUY4NgFjcwEBYWwBbGF1VudC5wb3VsYWluQGdtYWlsLmNvbQFzYwFkZXNrdG9wX3dLygFmcwFoc0lUMVlSYV9rTW0BendU1rL2FCQTdF&af=JnRzPTE1MjY2MTI3NzQmcHM9R3RRc29JUjg4VUNMWUxaUGRQTHVqZy0t; F=d=kXEUmFY9v1l3PWrKP3x4NQnfra1Ns38dBNW52XJ1.J2kL64GRr_eVfw5pttAJ; PH=fn=jMaW7R5RKV_kafaactc0xw--l=en-US&i=us; Y=v=1&n=0vck8js7k6l91&l=qy13tr5wzv0sxqxut5usyt1xuxrxz/o&p=0270000000000000&r=qp&lg=en-US&intl=us; SSL=1&s=iXHoGwlqfuI2PD_CmhueyGGheVPLbFzcEmoXHamQKg.KqKdUyTUeZE6si5hM6nNViIZeg_kBrDxbdjDCZg--&kv=0&ku=gESi0.LTzgIuVYSFNsjm_T6KxVycxb3SJfg0rAcQeY650NxPXwYD_tjexhVeVl7GgVepHPh2Hs1mtnSrok_XFxIt4HrZFRP2Ms04BEaFuaZJui0tL1Mf8U7Uf0HKhg0Sc8bFg34o.5fT.v8WP6R_L1Kdr0ULkXtueM0Ah4~A; A0=u=1; GUC=AQEEAQJa_49b0kIhNgTl&s=AQAAACZ2cFTs&g=Wv5DNQ

No request content (press tab to view response)

[143/159] [showhost] [transparent]
Warn: 10.10.0.106:55455: Client Handshake failed. The client may not trust t...(more in event)

3:24 / 3:27

Is 2FA useless?

- 2FA may not protect against a real-time attack
 - MITM attack
 - Phishing Website
- 2FA *is* effective if hackers get your password through a leak / key logger / camera
- FIDO security key seems to be resistant to a real-time attack (I did not try Bluetooth)

Universal 2nd Factor (U2F) using FIDO keys



Google Advanced Protection Program

- Designed for journalists, activists and high-value targets
- Second factor is *only* a FIDO key
- Second factor required after a logout / login
- Limits what can third-party apps access
- Account recovery can take a few days

Google second factor customization

- A good compromise between the super-strict Advanced Protection Program and a weak 2FA
- You can pick and choose your second factor(s)

2-Step Verification

Set up alternative second step

Set up at least one backup option so that you can sign in even if your other second steps aren't available.



Google prompt

Get a Google prompt on your phone and just tap **Yes** to sign in.

[ADD PHONE](#)



Authenticator app

Use the Authenticator app to get free verification codes, even when your phone is offline.
Available for Android and iPhone.

[SET UP](#)



Backup phone

Add a backup phone so you can still sign in if you lose your phone.

[ADD PHONE](#)



Security Key

A Security Key is a small physical device used for signing in. It plugs into your computer's USB port. [Learn more](#)

[ADD SECURITY KEY](#)

Check your account's recovery process

- How hard or easy is it for a bad guy to reset your password?
- How hard or easy is it for YOU to login after a catastrophe (e.g. theft, fire, accident)
- An authenticator app cannot be recovered if the phone is lost or destroyed

2FA security ranking

1. Google Advanced Protection Program
2. FIDO physical key
3. Non-SMS based app: vulnerable to realtime attack
4. SMS-based: vulnerable to realtime attack AND SIM hijacking

Questions?