SECURITY (COMP0141):
AUTHENTICATION ATTACKS

A RECENT PHISHING EMAIL

Metropolitan Police uk <d.j.ashley@comcast.net>

Dear Beneficiary;

My name is Inspector William Park, am working as the Head of Investigation with METROPOLITAN POLICE DEPARTMENT. there is presently a counter claims on your funds by one MR. BRENT STEVEN, who is presently trying to make us believe that you are dead and even explained that you entered into an agreement with him before your death, to help you in receiving your fund US$10,500,000.00 So here comes the big question.
Did you sign any Deed of Assignment in favor of (BRENT STEVEN), He further claimed that you died on the 9/MARCH/2019 and you have been buried, thereby making him the current beneficiary with his following account details:

ACCOUNT NAME: BRENT STEVEN
AC/NUMBER: 63758742.
ROUTING NUMBER: 122006743,
BANK NAME : FIRST BANK OF AMERICA
ADDRESS: NEW YORK, USA,

We shall proceed to issue all payments details to the said Mr. Brent Steven, if we do not hear from you within the next two working days from today. Are you truly dead as it was claimed by Mr. Brent Steven. You should also provide us with your direct telephone number where we can reach you today and what time we can get you on telephone.

If you are still alive you should contact the bank immediately.
Reply back ASAP.

Best Regards
Inspector Mike Lucas

PHISHING

By Victim Loss

Crime Type	Loss	Crime Type	Loss
BEC/EAC	$1,776,549,688	Employment	$42,618,705
Confidence Fraud/Romance	$475,014,032	Civil Matter	$20,242,867
Spoofing	$300,478,433	Harassment/Threats of Violence	$19,866,654
Investment	$222,186,195	Misrepresentation	$12,371,573
Real Estate/Rental	$221,365,911	IPR/Copyright and Counterfeit	$10,293,307
Non-Payment/Non-Delivery	$196,563,497	Ransomware	**$8,965,847
Identity Theft	$160,305,789	Denial of Service/TDoS	$7,598,198
Government Impersonation	$124,292,606	Charity	$2,214,383
Personal Data Breach	$120,102,501	Malware/Scareware/ Virus	$2,009,119
Credit Card Fraud	$111,491,163	Re-shipping	$1,772,692
Extortion	$107,498,956	Gambling	$1,458,118
Advanced Fee	$100,602,297	Health Care Related	$1,128,838
Other	$66,223,160	Crimes Against Children	$975,311
Phishing/Vishing/Smishing/Pharming	$57,836,379	Hacktivist	$129,000
Overpayment	$55,820,212	Terrorism	$49,589
Tech Support	$54,041,053		
Corporate Data Breach	$53,398,278		
Lottery/Sweepstakes/Inheritance	$48,642,332		

PHISHING AND FRIENDS

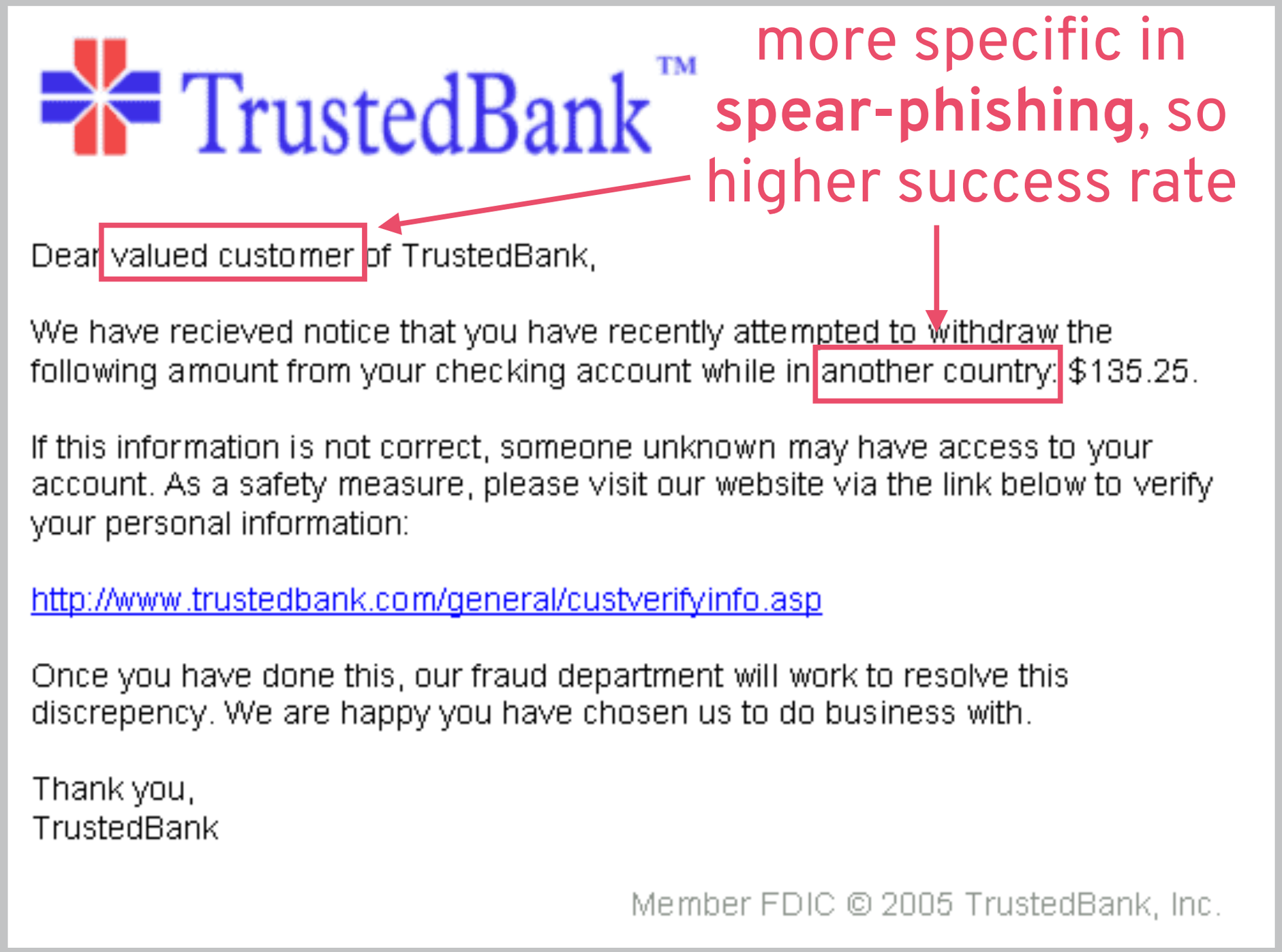
Phishing happens via email

Vishing happens over the phone (“voice phishing”) - can use deepfake techniques to perform impersonation

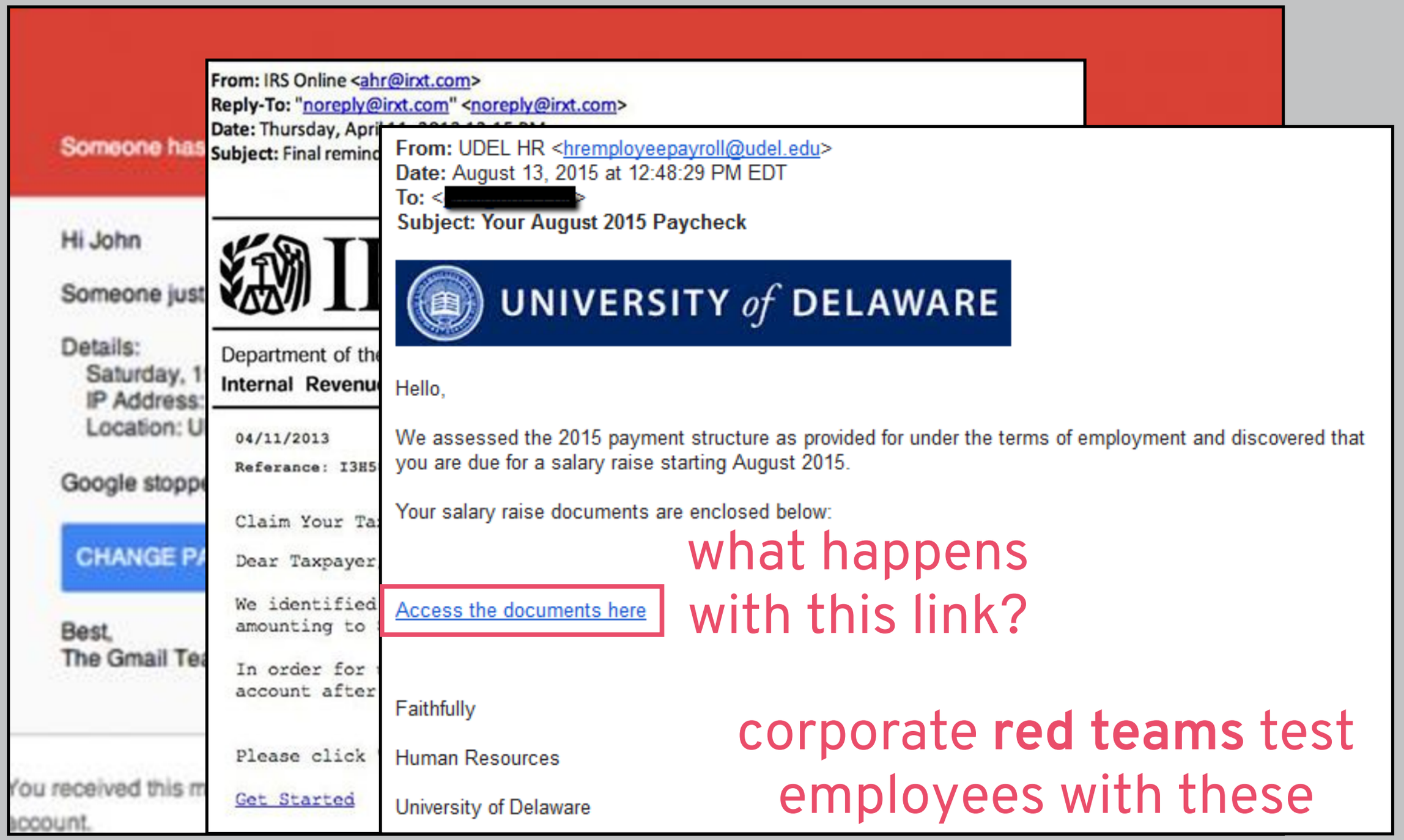
Smishing happens via SMS

Pharming is a technique to enhance phishing

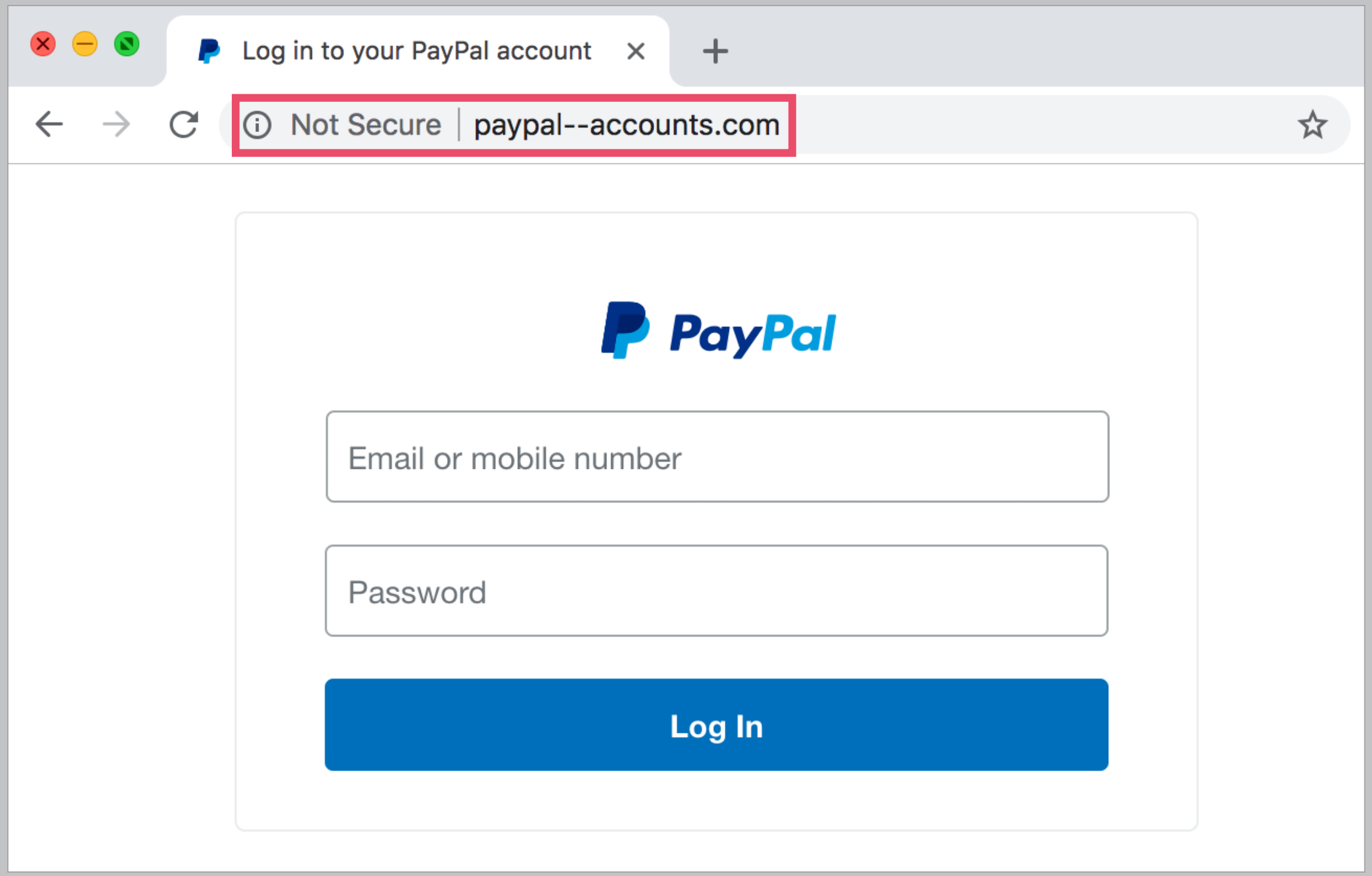
PHISHING


TrustedBank™
more specific in **spear-phishing**, so higher success rate
Dear valued customer of TrustedBank,
We have recieved notice that you have recently attempted to withdraw the following amount from your checking account while in another country: $135.25.
If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:
http://www.trustedbank.com/general/custverifyinfo.asp
Once you have done this, our fraud department will work to resolve this discrepency. We are happy you have chosen us to do business with.
Thank you,
TrustedBank
Member FDIC © 2005 TrustedBank, Inc.

SPEAR-PHISHING



A PHISHING WEBSITE



WRONG URLS/TYPOSQUATTING

http://www.secure-trustedbank.com/

http://www.trustedbank.com@evilsite.com/

http://www.trustedbank.com@72.167.76.127/

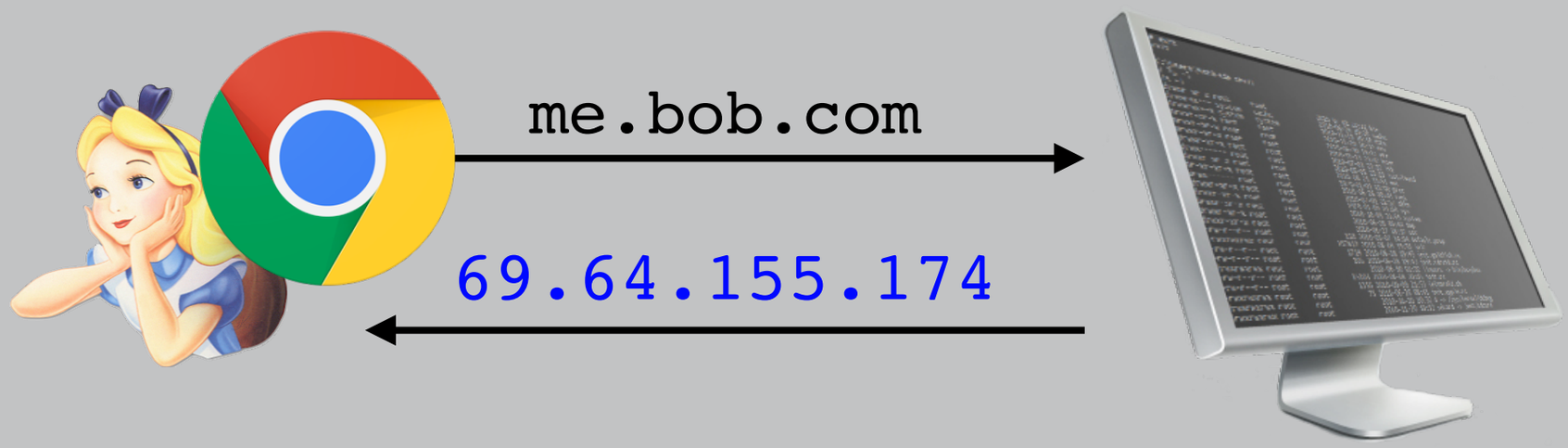
irrelevant if attacker owns domain!

http://www.steamcomrnunity.com/

http://www.lioydsbank.com/

also used for other nefarious purposes
(drive-by downloads, ad revenue, etc.)

PHARMING



alice.com	174.123.32.42
me.bob.com	192.220.74.179
…	…

OTHER ATTACKS ON ‘WHAT YOU KNOW’

Capture attacks:

- Skimming (works for PINs)
- Keylogging
- Packet sniffing (unencrypted web traffic)

Intimate partner violence (attacker doesn’t need to guess)

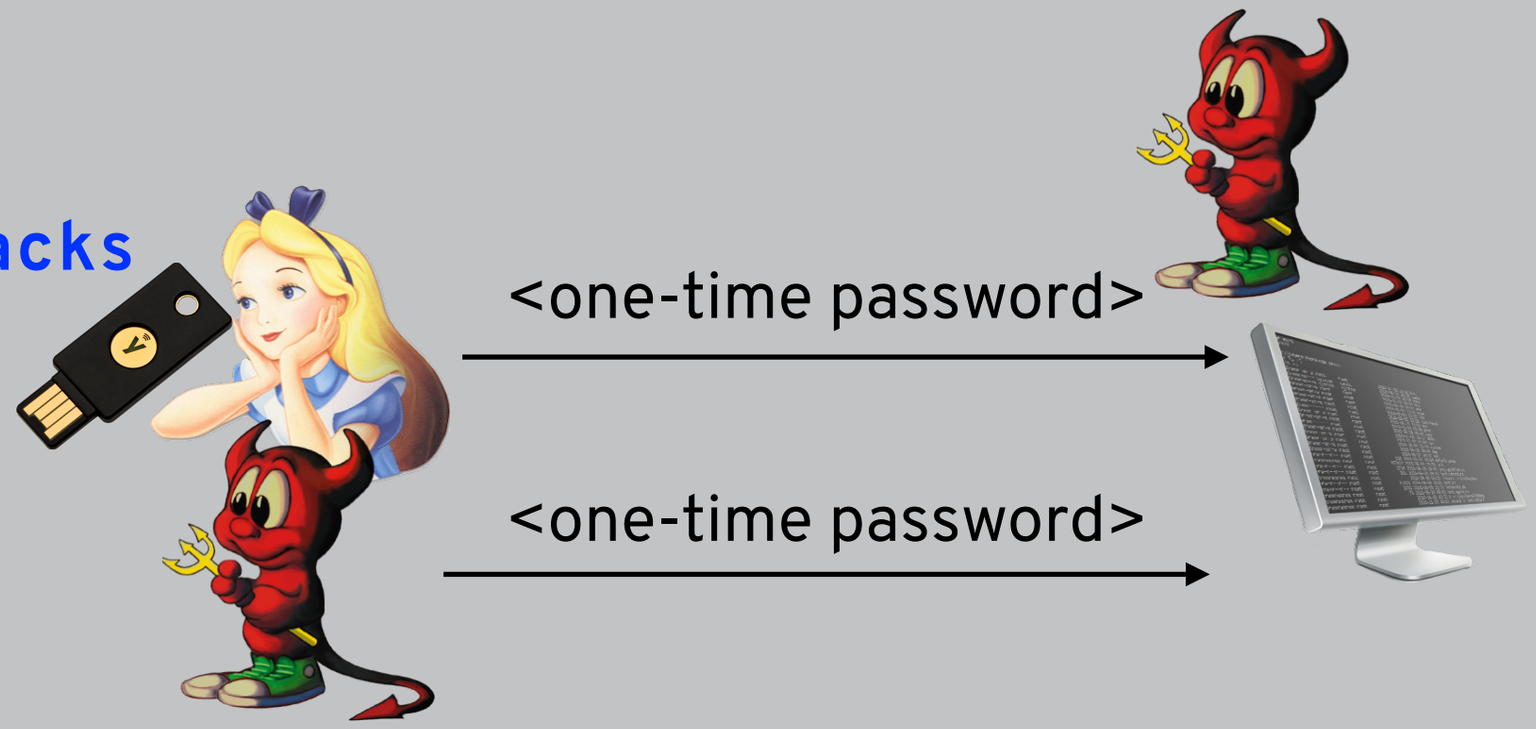
Observation attacks (shoulder-surfing)

Side-channel attacks (keyboard emanations, finger grease)

Coercion (“rubber-hose”) attacks

ATTACKS ON ‘WHAT YOU HAVE’

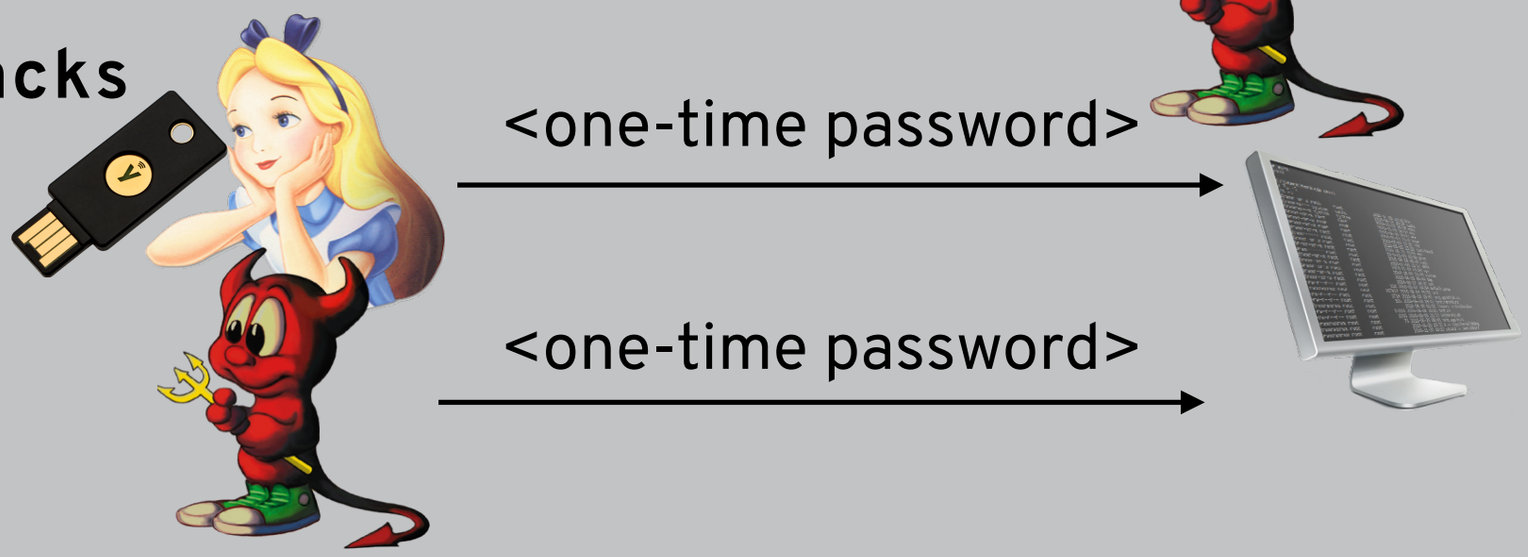
Replay attacks



Classic but easily prevented using session IDs (for example)

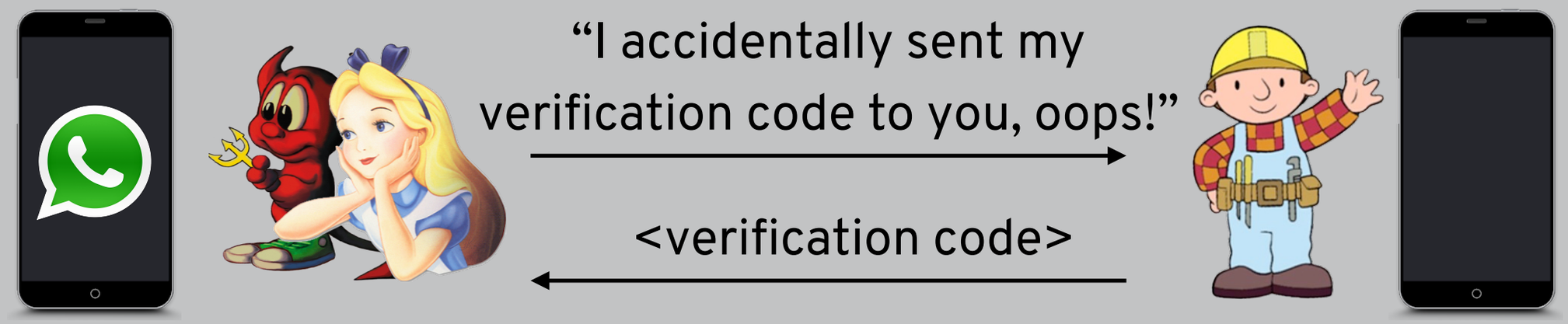
ATTACKS ON ‘WHAT YOU HAVE’

Replay attacks



Classic but easily prevented using session IDs (for example)

Verification scams



...registers Bob’s number...

...gets verification SMS...

HAVE I BEEN PWNED? (DEMO)

PASSWORD REUSE

If your Hotmail password is compromised, this has obvious implications for your Hotmail account security

What about your Github account? Gmail?

How many different accounts do you have (N)? How many different passwords (M)? Is N ≫ M? 👀

CREDENTIAL STUFFING

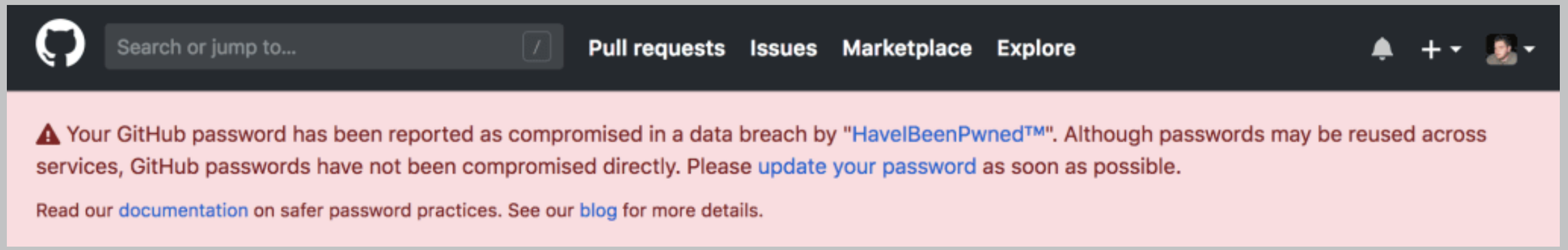
rockyou.txt

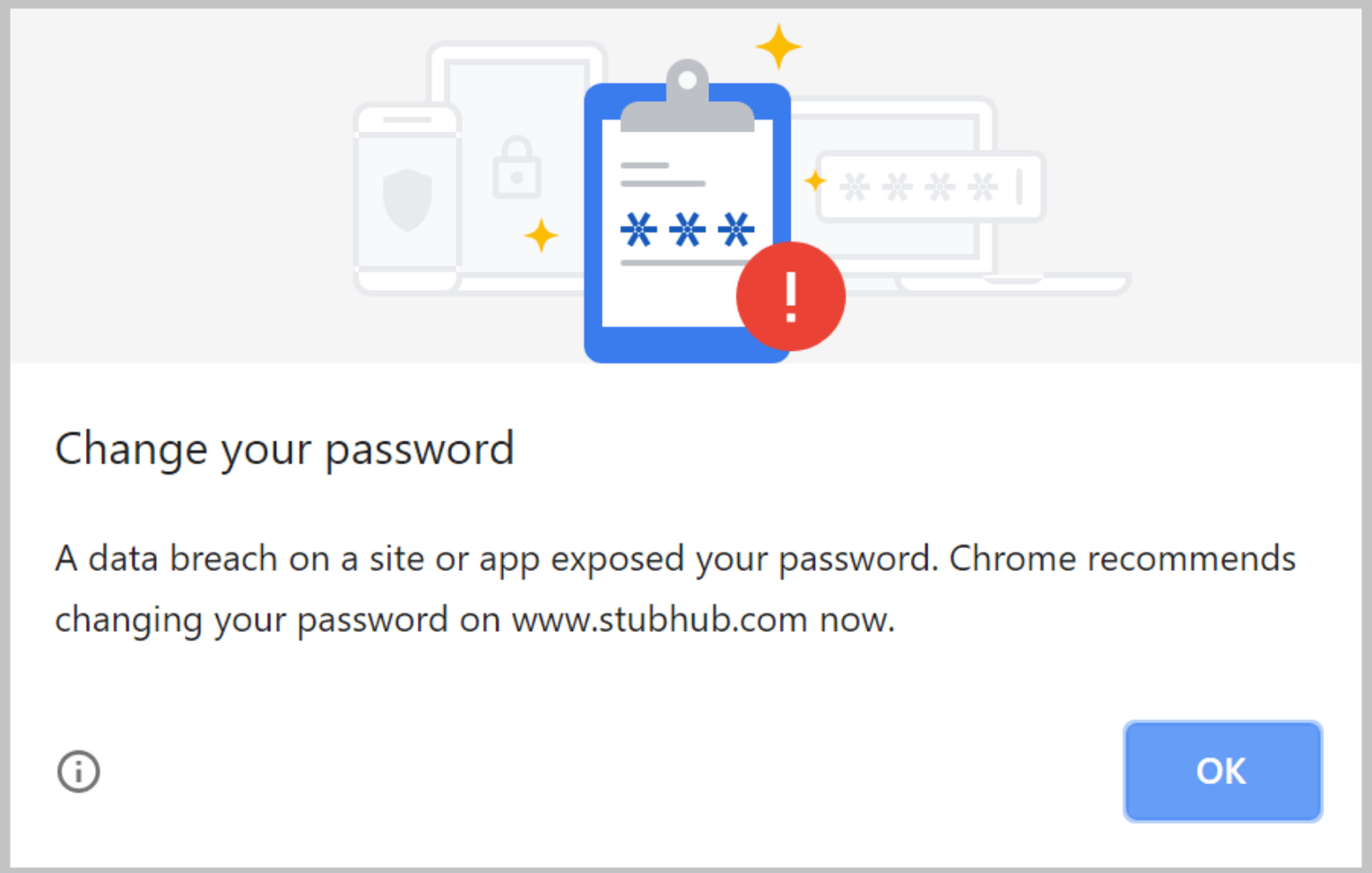
u1	p1
u2	p2
...	...
un	pn

ui, pi

credential tweaking is a more sophisticated attack in which attacker applies mangling rules (like JtR)

WARNINGS


Search or jump to...
/
Pull requests
Issues
Marketplace
Explore
Your GitHub password has been reported as compromised in a data breach by "HaveIBeenPwned™". Although passwords may be reused across services, GitHub passwords have not been compromised directly. Please update your password as soon as possible.
Read our documentation on safer password practices. See our blog for more details.


Change your password
A data breach on a site or app exposed your password. Chrome recommends changing your password on www.stubhub.com now.
OK

SOLUTIONS

Password cracking is an **offline guessing attack**: have as many guesses as your hardware/patience allows

Credential stuffing is an **online guessing attack**: have as many guesses as the platform allows before locking account

- Too permissive? Higher risk of the attacker succeeding
- Too strict? Higher risk of the (real) user getting locked out

PASSWORD REUSE

If your Hotmail password is compromised, this has obvious implications for your Hotmail account security

What about your Github account? Gmail?

How many different accounts do you have (N)? How many different passwords (M)? Is N ≫ M? 👀

Password managers ensure that N = M

(but have their own set of issues!)

ACCESS CONTROL

uname,passwd

“give me Bob’s file”

still need to ensure **access control**

“open Bob’s unit”

QUIZ!

Please go to

`https://moodle.ucl.ac.uk/mod/quiz/view.php?id=2833302`

to take this week's quiz!