C -> S: **GET http://www.example.com/**

S -> C: page, including a login form

C -> S: **GET http://www.example.com/login?**
u=USER&p=PASSWD

[server marks this session as authenticated]

S -> C: **Set-Cookie: sessionid=***NONCE*

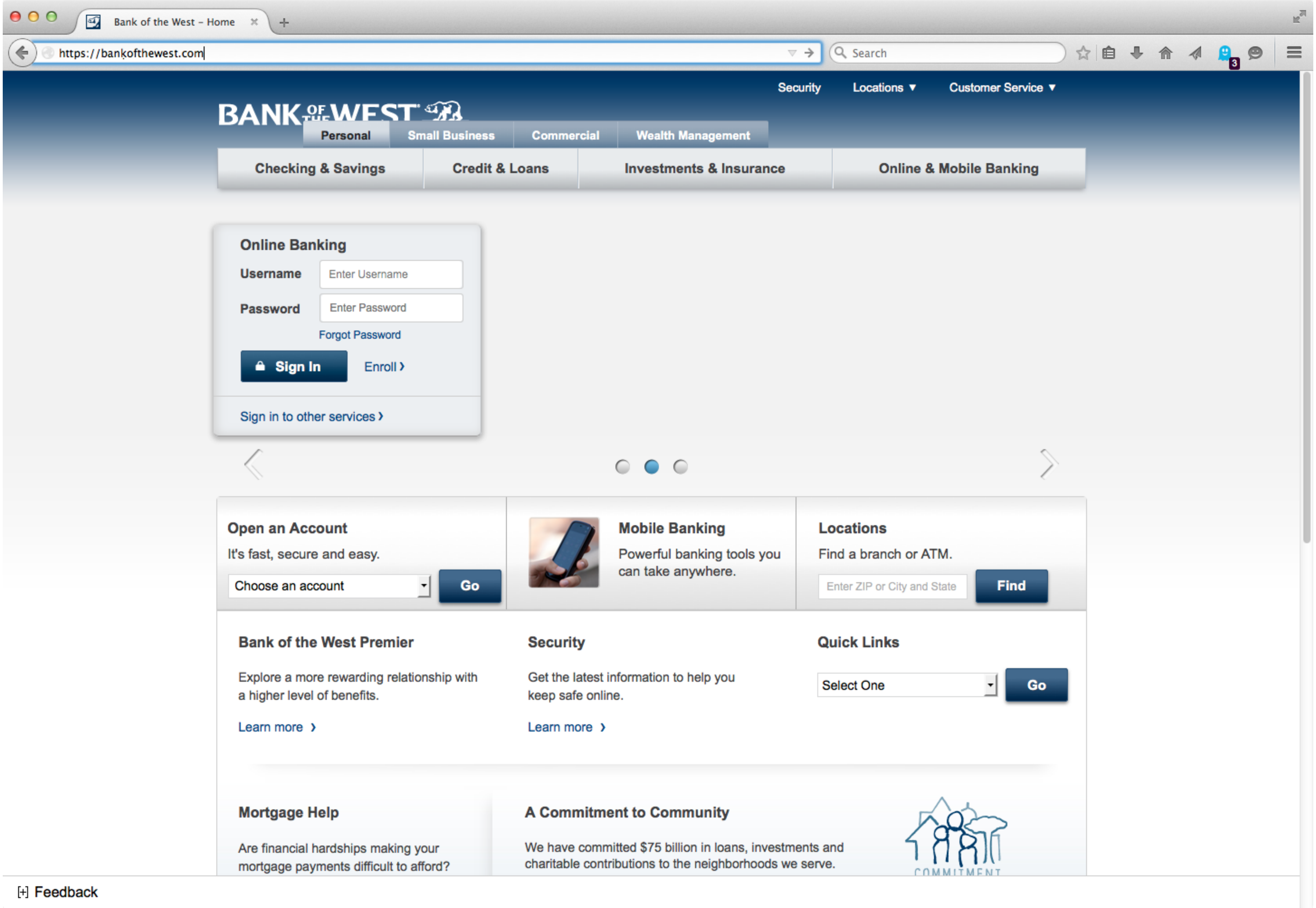
(Cookie is an "authenticator" for session)

C -> S: **GET http://www.example.com/somepage**
Cookie: sessionid=*NONCE*

```
<img src="http://bank.example/withdraw?
account=bob&amount=1000000&for=mallory">
```

Challenges

- MITM
  - Network
  - Proxy/relay
- “Transaction generators” / malware
  - Parasitic on communication
- Mobility
  - Multiple devices
- Impatient/Untrainable Users



Online Banking

Username

Password

Forgot Password

Enroll ›

Sign in to other services ›

Open an Account

It's fast, secure and easy.

Mobile Banking

Powerful banking tools you can take anywhere.

Locations

Find a branch or ATM.

Bank of the West Premier

Explore a more rewarding relationship with a higher level of benefits.

Learn more ›

Security

Get the latest information to help you keep safe online.

Learn more ›

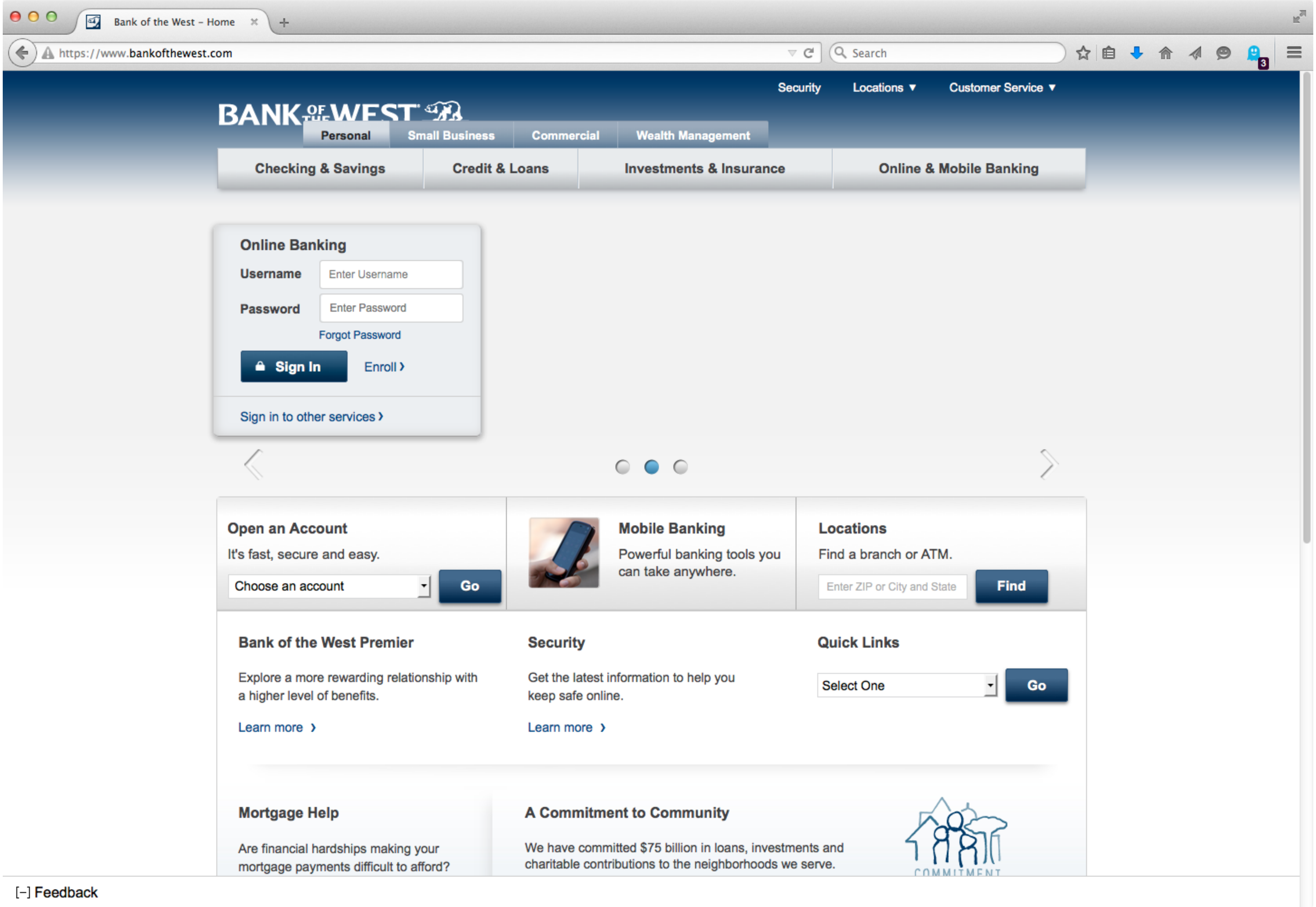
Quick Links

Mortgage Help

Are financial hardships making your mortgage payments difficult to afford?

A Commitment to Community

We have committed $75 billion in loans, investments and charitable contributions to the neighborhoods we serve.



Online Banking

Username: Enter Username

Password: Enter Password

Open an Account

It's fast, secure and easy.

Mobile Banking

Powerful banking tools you can take anywhere.

Locations

Find a branch or ATM.

Bank of the West Premier

Explore a more rewarding relationship with a higher level of benefits.

Security

Get the latest information to help you keep safe online.

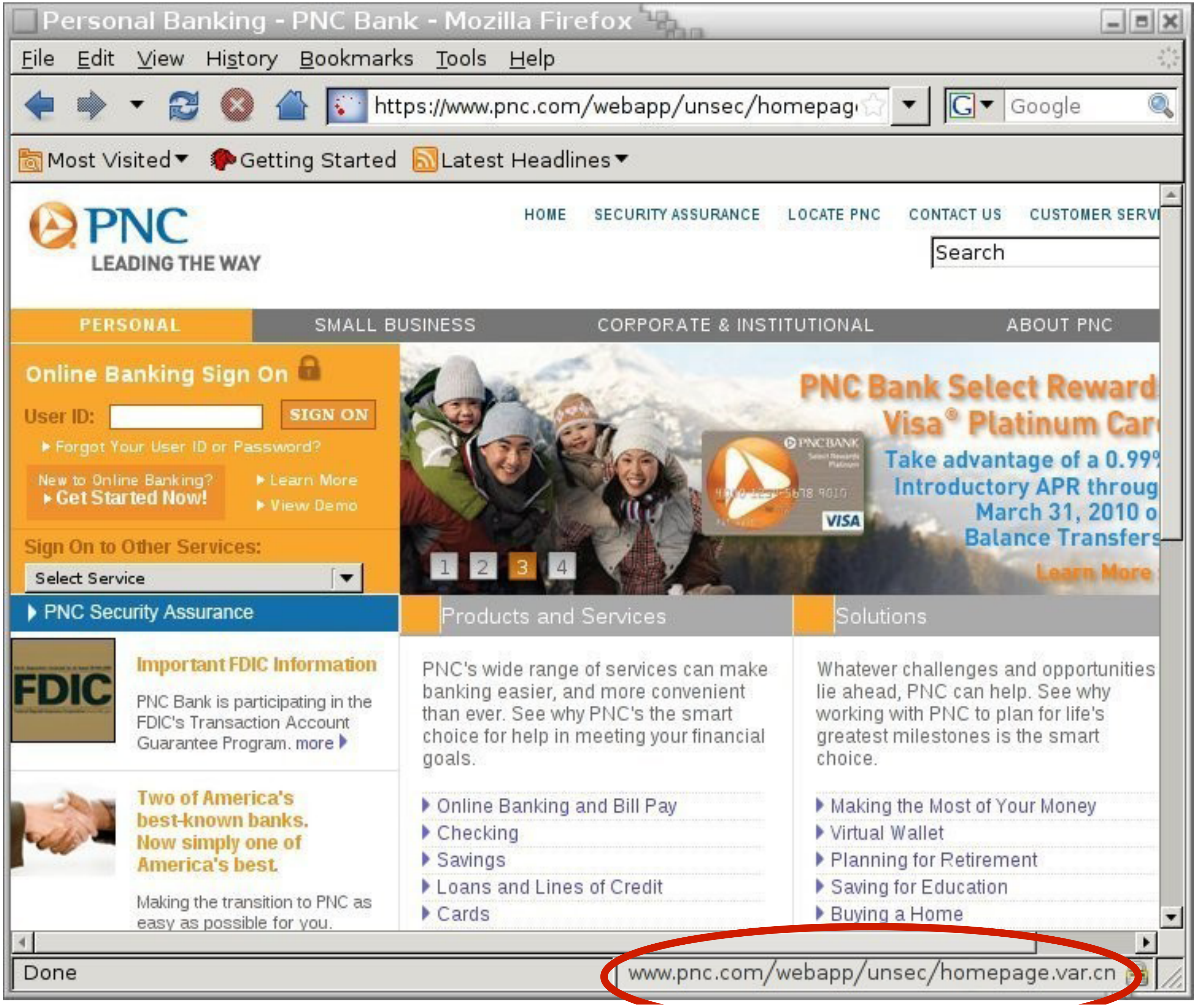
Quick Links

Mortgage Help

Are financial hardships making your mortgage payments difficult to afford?

A Commitment to Community

We have committed $75 billion in loans, investments and charitable contributions to the neighborhoods we serve.



Personal Banking - PNC Bank - Mozilla Firefox

PNC Bank Select Reward
Visa® Platinum Car
Take advantage of a 0.99
Introductory APR throug
March 31, 2010 o
Balance Transfers
Learn More

Important FDIC Information

PNC Bank is participating in the FDIC's Transaction Account Guarantee Program. more

Two of America's best-known banks. Now simply one of America's best.

Making the transition to PNC as easy as possible for you.

PNC's wide range of services can make banking easier, and more convenient than ever. See why PNC's the smart choice for help in meeting your financial goals.

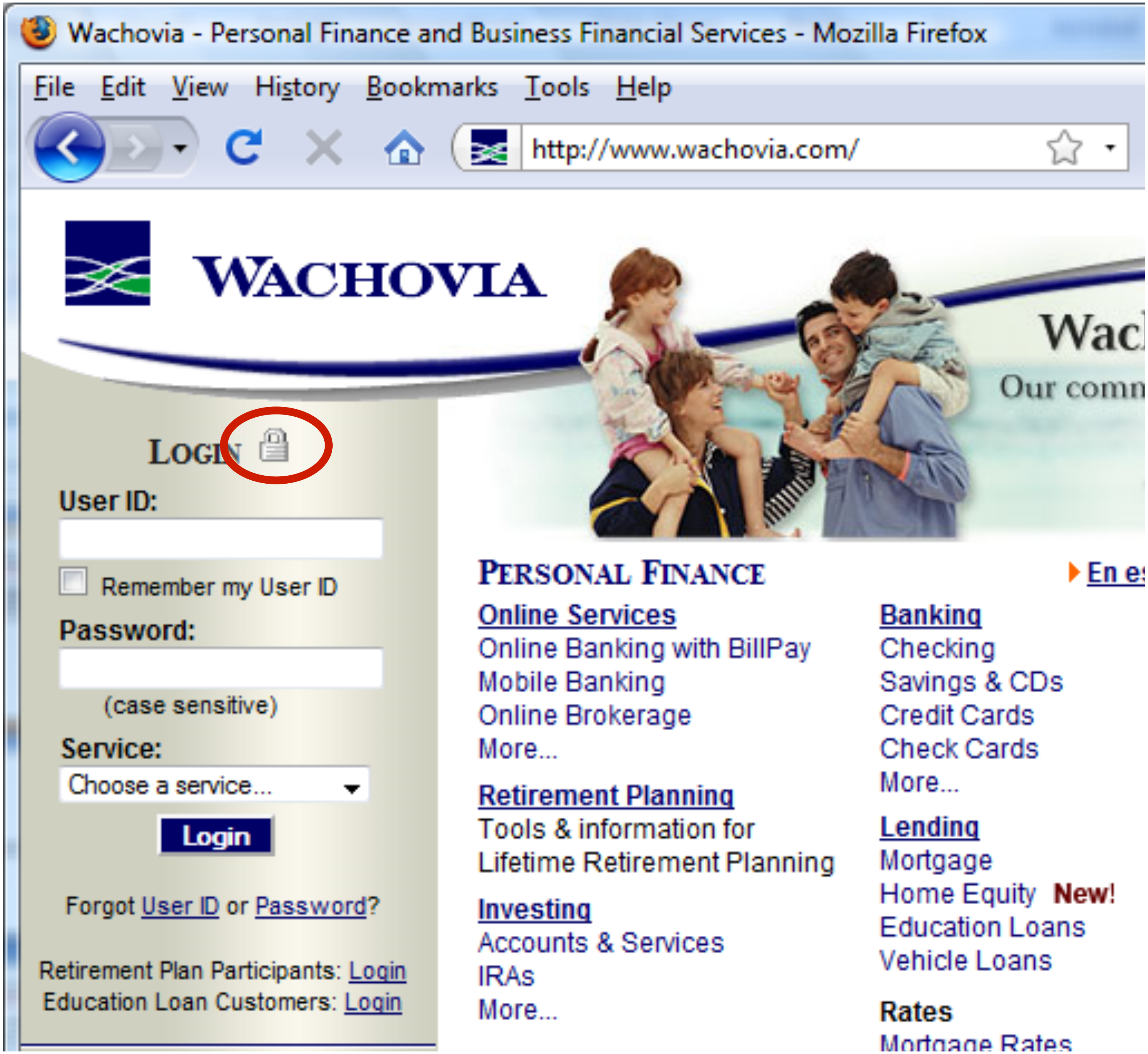
- Online Banking and Bill Pay
- Checking
- Savings
- Loans and Lines of Credit
- Cards

Whatever challenges and opportunities lie ahead, PNC can help. See why working with PNC to plan for life's greatest milestones is the smart choice.

- Making the Most of Your Money
- Virtual Wallet
- Planning for Retirement
- Saving for Education
- Buying a Home

Done

www.pnc.com/webapp/unsec/homepage.var.cn



Wachovia - Personal Finance and Business Financial Services - Mozilla Firefox

http://www.wachovia.com/

WACHOVIA

Wac

Our comn

LOGIN

User ID:

□ Remember my User ID

Password:

(case sensitive)

Service:

Choose a service...

Forgot User ID or Password?

Retirement Plan Participants: Login
Education Loan Customers: Login

PERSONAL FINANCE

En es

Online Services
Online Banking with BillPay
Mobile Banking
Online Brokerage
More...

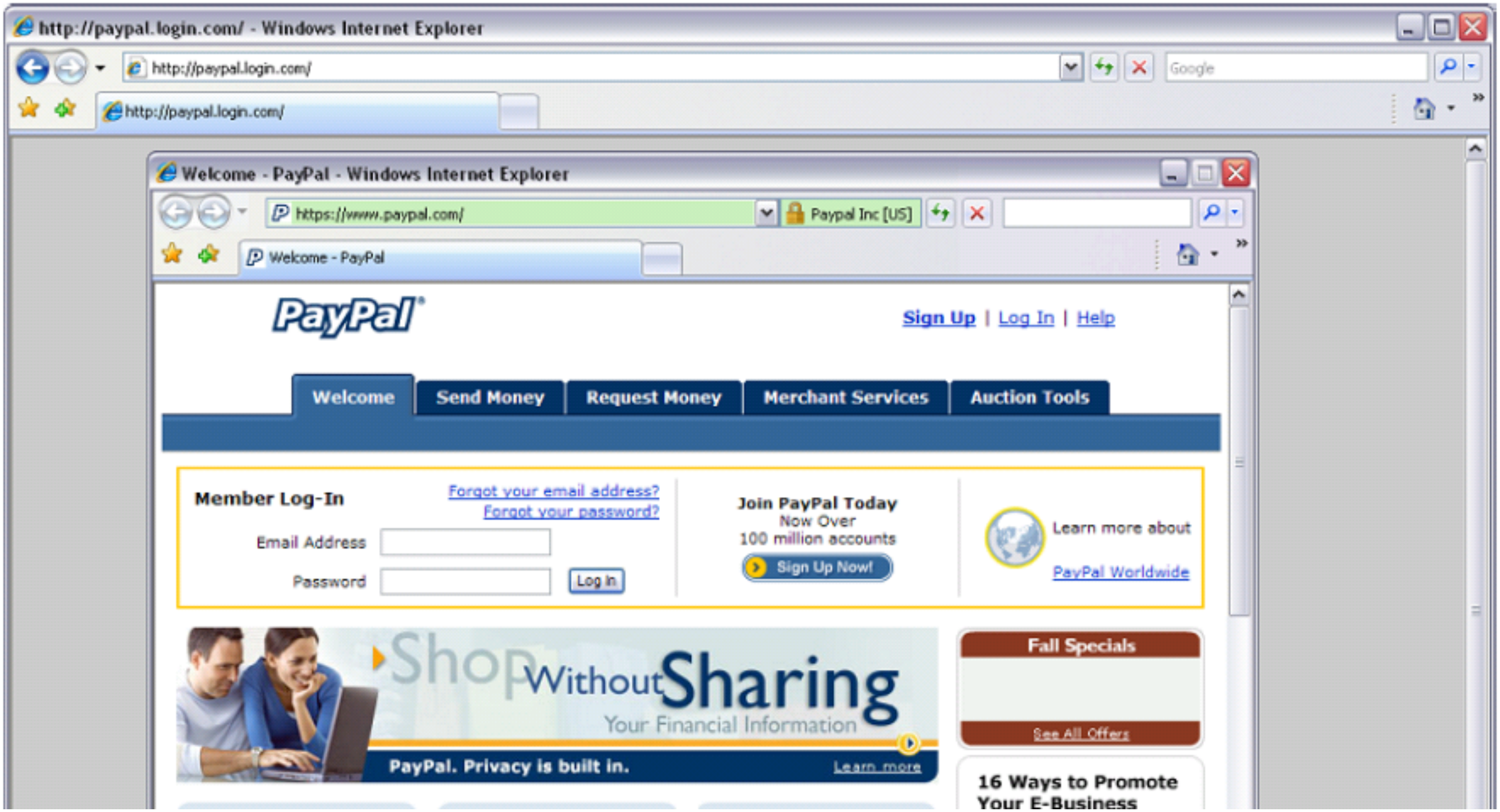
Retirement Planning
Tools & information for
Lifetime Retirement Planning

Investing
Accounts & Services
IRAs
More...

Banking
Checking
Savings & CDs
Credit Cards
Check Cards
More...

Lending
Mortgage
Home Equity New!
Education Loans
Vehicle Loans

Rates
Mortgage Rates



http://paypal.login.com/ - Windows Internet Explorer

http://paypal.login.com/

Welcome - PayPal - Windows Internet Explorer

https://www.paypal.com/

Paypal Inc [US]

Welcome - PayPal

Member Log-In

Email Address

Password

Join PayPal Today
Now Over
100 million accounts

Learn more about PayPal Worldwide

Shop Without Sharing Your Financial Information

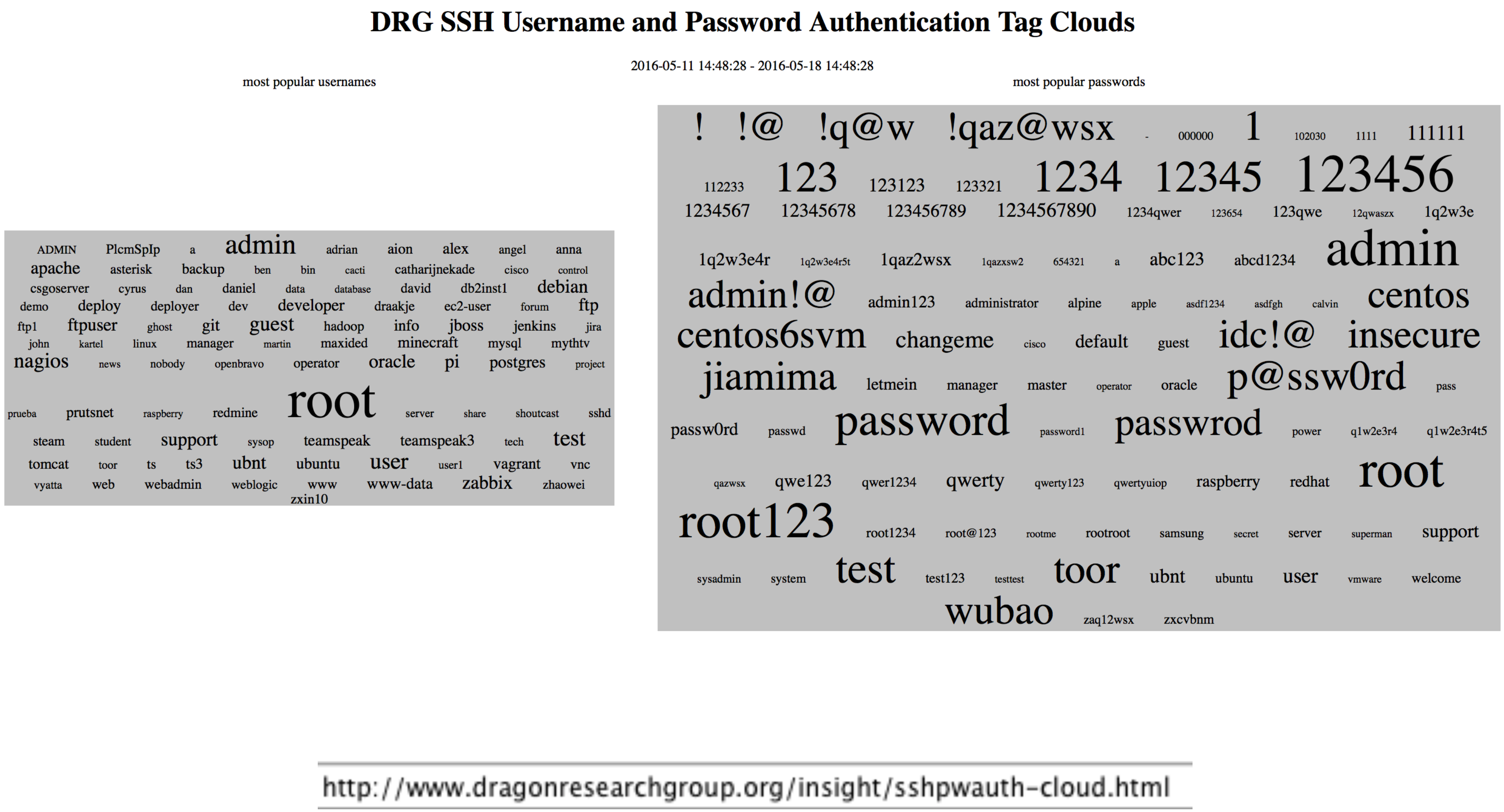
PayPal. Privacy is built in.

Fall Specials

16 Ways to Promote Your E-Business

Thinking about Passwords

- Big Web Service Provider perspective:
  - "*If you are using passwords for your services, you are screwed.*"
- Desired properties:
  - Easy to produce
  - Portability (use from different machines)
  - Scalability (can have lots of accounts)
- Tension with threats?



DRG SSH Username and Password Authentication Tag Clouds

2016-05-11 14:48:28 - 2016-05-18 14:48:28

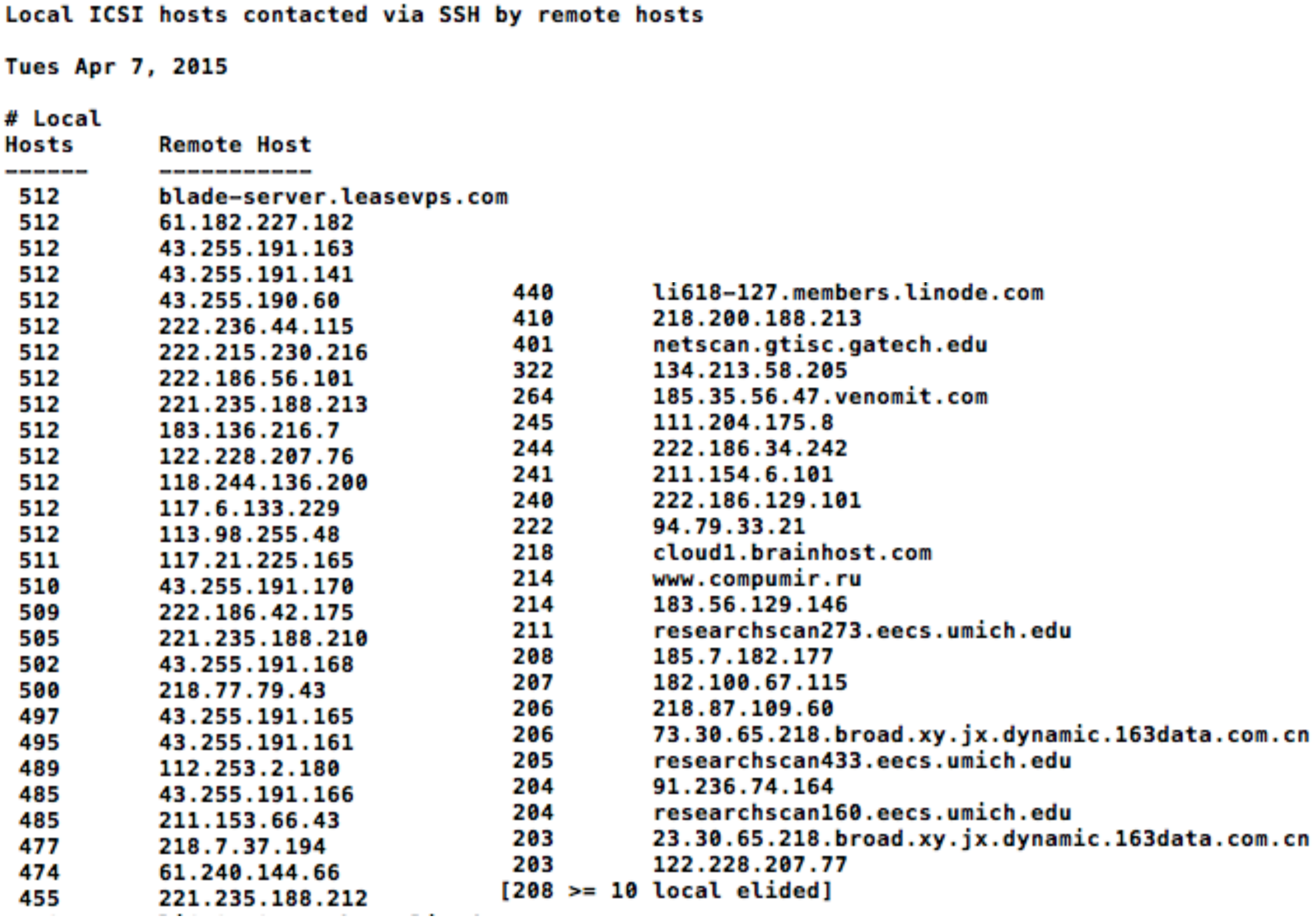
most popular usernames

ADMIN PlcmSpIp a admin adrian aion alex angel anna
apache asterisk backup ben bin cacti catharijnekade cisco control
csgoserver cyrus dan daniel data database david db2inst1 debian
demo deploy deployer dev developer draakje ec2-user forum ftp
ftp1 ftpuser ghost git guest hadoop info jboss jenkins jira
john kartel linux manager martin maxided minecraft mysql mythtv
nagios news nobody openbravo operator oracle pi postgres project
prueba prutsnet raspberry redmine root server share shoutcast sshd
steam student support sysop teamspeak teamspeak3 tech test
tomcat toor ts ts3 ubnt ubuntu user user1 vagrant vnc
vyatta web webadmin weblogic www www-data zabbix zhaowei
zxin10

most popular passwords

! !@ !q@w !qaz@wsx - 000000 1 102030 1111 111111
112233 123 123123 123321 1234 12345 123456
1234567 12345678 123456789 1234567890 1234qwer 123654 123qwe 12qwaszx 1q2w3e
1q2w3e4r 1q2w3e4r5t 1qaz2wsx 1qazxsw2 654321 a abc123 abcd1234 admin
admin!@ admin123 administrator alpine apple asdf1234 asdfgh calvin centos
centos6svm changeme cisco default guest idc!@ insecure
jiamima letmein manager master operator oracle p@ssw0rd pass
passw0rd passwd password password1 passwrod power q1w2e3r4 q1w2e3r4t5
qazwsx qwe123 qwer1234 qwerty qwerty123 qwertyuiop raspberry redhat root
root123 root1234 root@123 rootme rootroot samsung secret server superman support
sysadmin system test test123 testtest toor ubnt ubuntu user vmware welcome
wubao zaq12wsx zxcvbnm

http://www.dragonresearchgroup.org/insight/sshpwauth-cloud.html

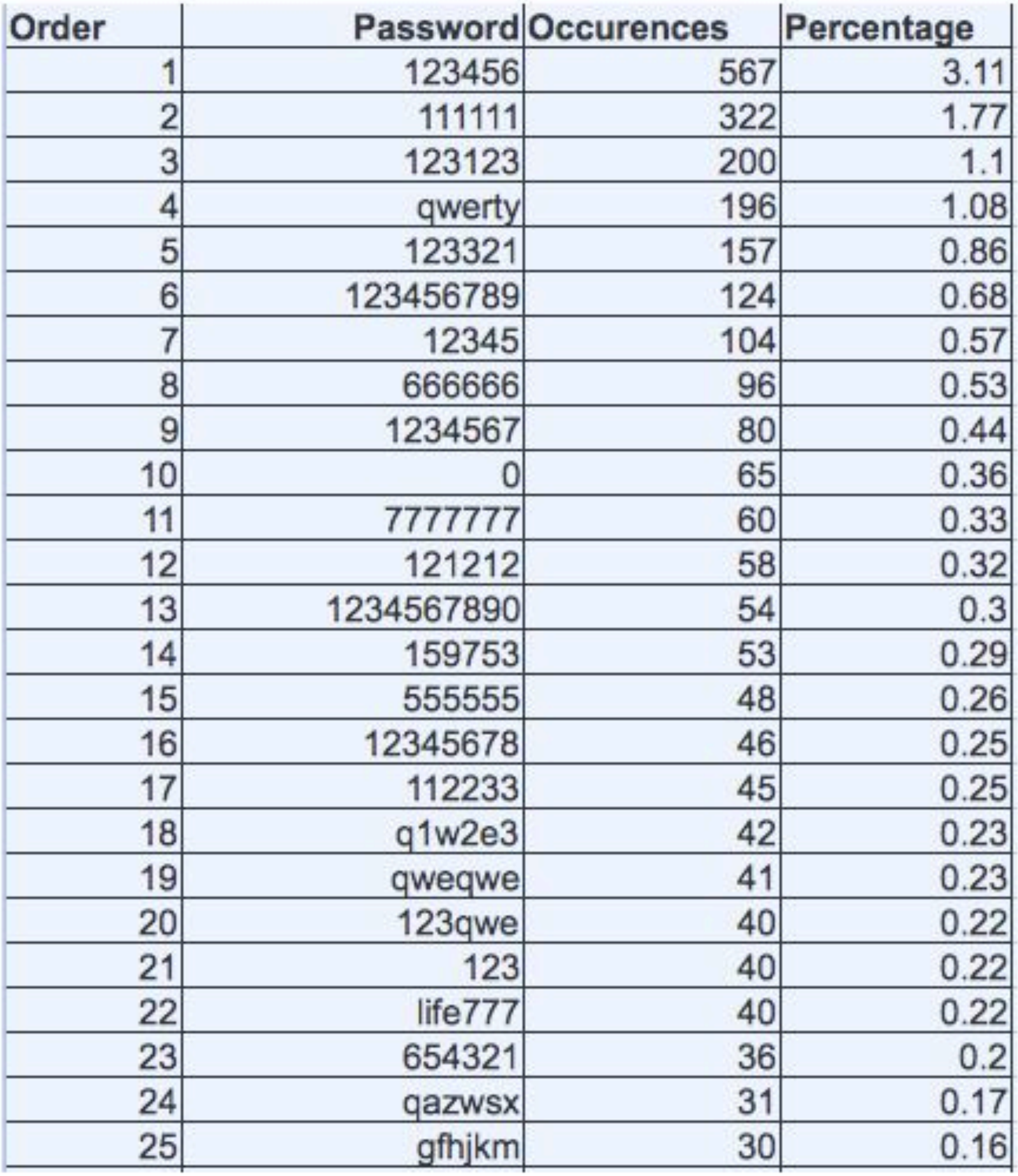


```
Local ICSI hosts contacted via SSH by remote hosts

Tues Apr 7, 2015

# Local
Hosts     Remote Host
------    -----------
 512      blade-server.leasevps.com
 512      61.182.227.182
 512      43.255.191.163
 512      43.255.191.141
 512      43.255.190.60
 512      222.236.44.115
 512      222.215.230.216
 512      222.186.56.101
 512      221.235.188.213
 512      183.136.216.7
 512      122.228.207.76
 512      118.244.136.200
 512      117.6.133.229
 512      113.98.255.48
 511      117.21.225.165
 510      43.255.191.170
 509      222.186.42.175
 505      221.235.188.210
 502      43.255.191.168
 500      218.77.79.43
 497      43.255.191.165
 495      43.255.191.161
 489      112.253.2.180
 485      43.255.191.166
 485      211.153.66.43
 477      218.7.37.194
 474      61.240.144.66
 455      221.235.188.212

 440      li618-127.members.linode.com
 410      218.200.188.213
 401      netscan.gtisc.gatech.edu
 322      134.213.58.205
 264      185.35.56.47.venomit.com
 245      111.204.175.8
 244      222.186.34.242
 241      211.154.6.101
 240      222.186.129.101
 222      94.79.33.21
 218      cloud1.brainhost.com
 214      www.compumir.ru
 214      183.56.129.146
 211      researchscan273.eecs.umich.edu
 208      185.7.182.177
 207      182.100.67.115
 206      218.87.109.60
 206      73.30.65.218.broad.xy.jx.dynamic.163data.com.cn
 205      researchscan433.eecs.umich.edu
 204      91.236.74.164
 204      researchscan160.eecs.umich.edu
 203      23.30.65.218.broad.xy.jx.dynamic.163data.com.cn
 203      122.228.207.77
[208 >= 10 local elided]
```



Order	Password	Occurences	Percentage
1	123456	567	3.11
2	111111	322	1.77
3	123123	200	1.1
4	qwerty	196	1.08
5	123321	157	0.86
6	123456789	124	0.68
7	12345	104	0.57
8	666666	96	0.53
9	1234567	80	0.44
10	0	65	0.36
11	7777777	60	0.33
12	121212	58	0.32
13	1234567890	54	0.3
14	159753	53	0.29
15	555555	48	0.26
16	12345678	46	0.25
17	112233	45	0.25
18	q1w2e3	42	0.23
19	qweqwe	41	0.23
20	123qwe	40	0.22
21	123	40	0.22
22	life777	40	0.22
23	654321	36	0.2
24	qazwsx	31	0.17
25	gfhjkm	30	0.16

"gee I hope 2 elephants don't step on me" "gIh2ed'tsom"

(1) Get victim's email & home (billing) address

(2) Call Amazon, say you're the victim & want to
add a credit card #

(2') Add bogus card

(3) Call Amazon: "I've lost access to my email account"
Provide name, billing addr, new credit card #

(3') Add new email account

(4) Go to Amazon web site, send password reset to new acct

(5) This reveals last four digits of account CCs

(6) Go to Apple. Provide billing addr & last 4 digits ...

(6') ... receive temporary iCloud password

(7) Go to N services, do password resets emailed to acct

(8) PROFIT

Effective Warnings

- Interrupt primary task
- Provide clear choices
- Fail safely (if user ignores / navigates away)
- Prevent habituation
- Alter site presentation (look & feel) if iffy

To: vern@ee.lbl.gov
Subject: RE: Russian spear phishing attack against .mil and .gov employees
From: jeffreyc@cia.gov
Date: Wed, 10 Feb 2010 19:51:47 +0100

Russian spear phishing attack against .mil and .gov employees

A "relatively large" number of U.S. government and military employees are being taken in by a spear phishing attack which delivers a variant of the Zeus trojan. The email address is spoofed to appear to be from the NSA or InteLink concerning a report by the National Intelligence Council named the "2020 Project". It's purpose is to collect passwords and obtain remote access to the infected hosts.

Security Update for Windows 2000/XP/Vista/7 (KB823988)

About this download: A security issue has been identified that could allow an attacker to remotely compromise a computer running Microsoft Windows and gain complete control over it. You can help protect your computer by installing this update from Microsoft. After you install this item, you may have to restart your computer.

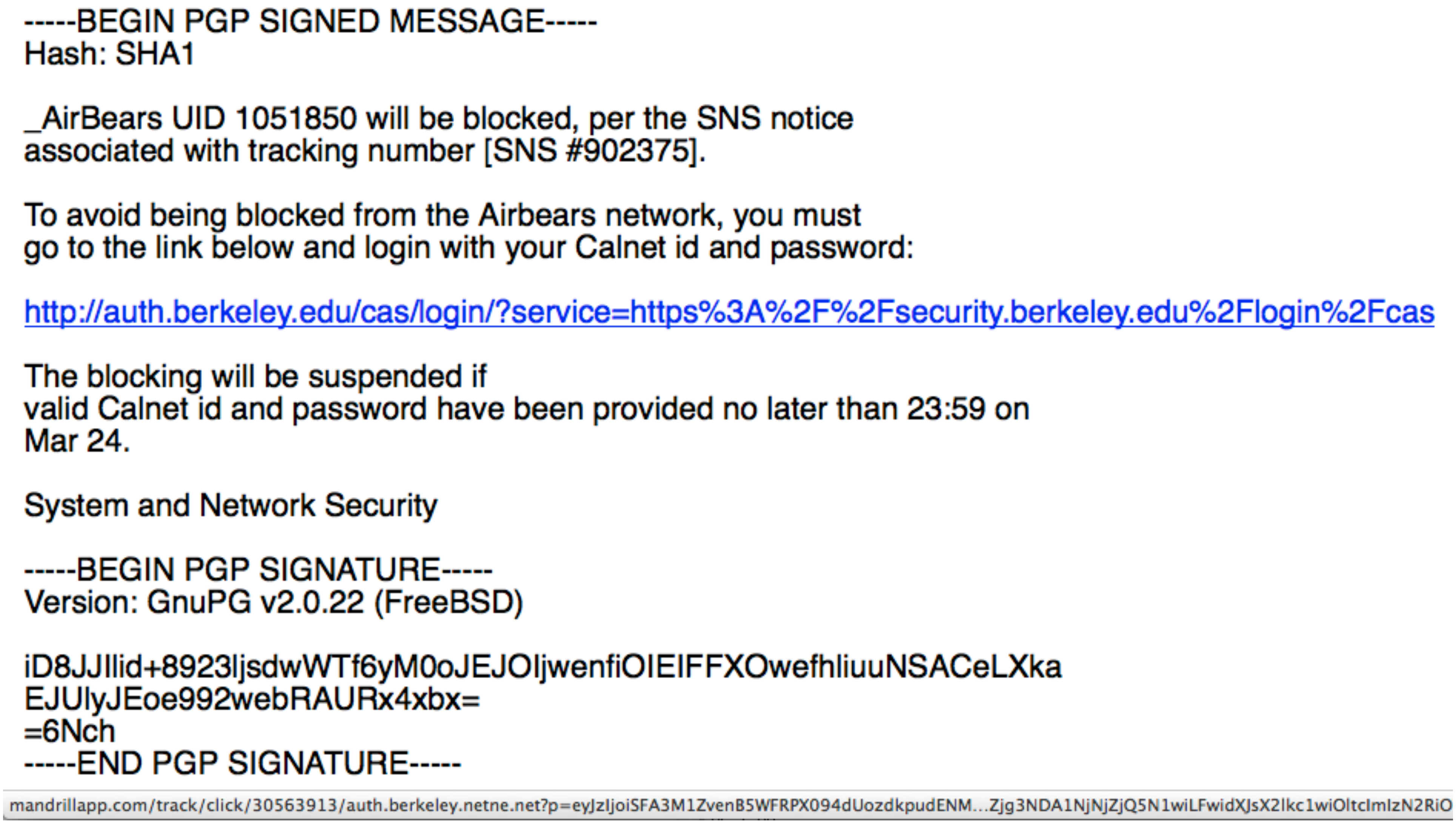
Download:

http://mv.net.md/update/update.zip

or

http://www.sendspace.com/file/xwc1pi

____
Jeffrey Carr is the CEO of GreyLogic, the Founder and Principal Investigator of Project Grey Goose, and the author of "Inside Cyber Warfare".
jeffreyc@greylogic.us



```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

_AirBears UID 1051850 will be blocked, per the SNS notice
associated with tracking number [SNS #902375].

To avoid being blocked from the Airbears network, you must
go to the link below and login with your Calnet id and password:

http://auth.berkeley.edu/cas/login/?service=https%3A%2F%2Fsecurity.berkeley.edu%2Flogin%2Fcas

The blocking will be suspended if
valid Calnet id and password have been provided no later than 23:59 on
Mar 24.

System and Network Security

-----BEGIN PGP SIGNATURE-----
Version: GnuPG v2.0.22 (FreeBSD)

iD8JJIlid+8923ljsdwWTf6yM0oJEJOIjwenfiOIEIFFXOwefhliuuNSACeLXka
EJUlyJEoe992webRAURx4xbx=
=6Nch
-----END PGP SIGNATURE-----
```

mandrillapp.com/track/click/30563913/auth.berkeley.netne.net?p=eyJzIjoiSFA3M1ZvenB5WFRPX094dUozdkpudENM...Zjg3NDA1NjNjZjQ5N1wiLFwidXJsX2lkc1wiOltcImIzN2RiO

The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes*

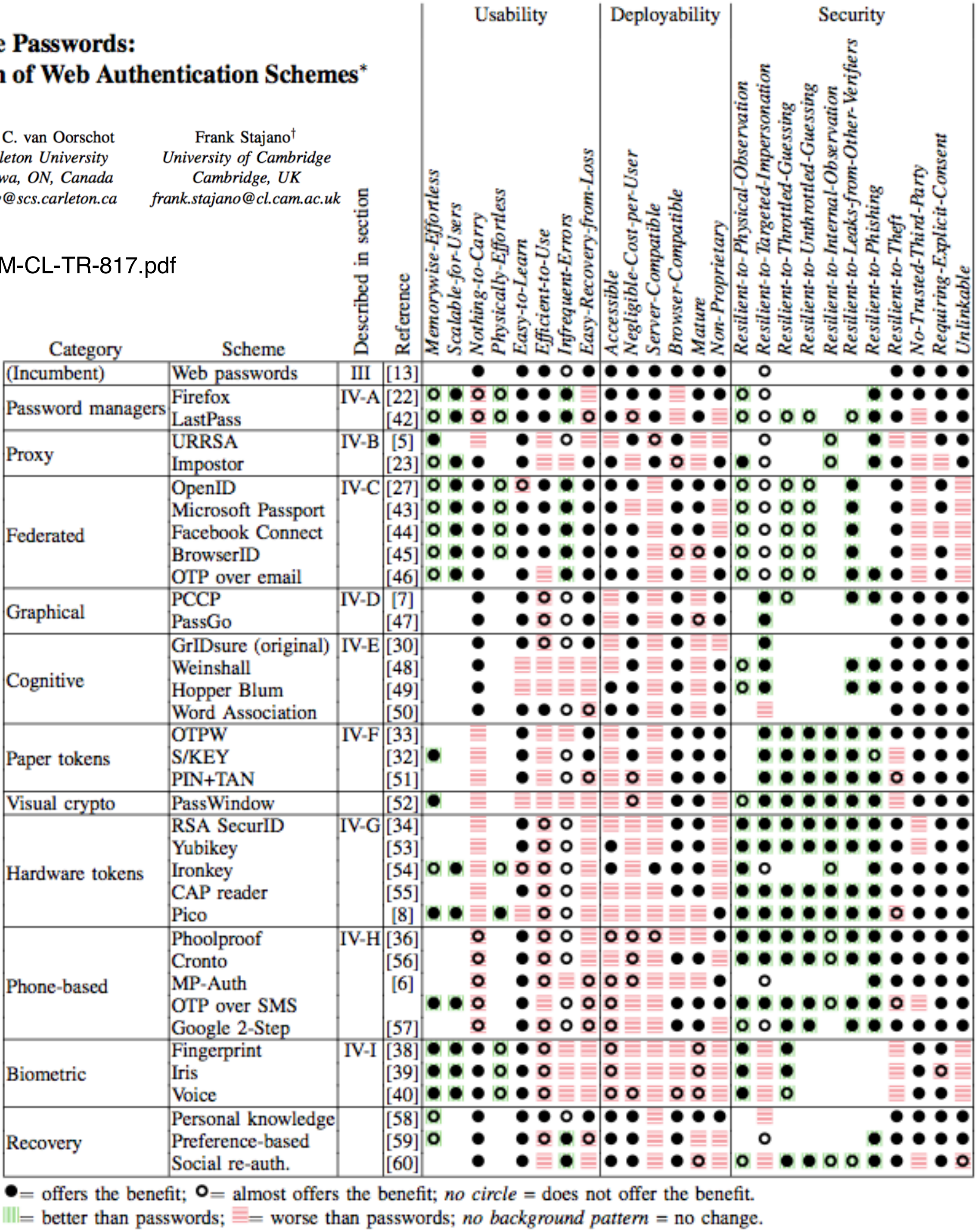
Joseph Bonneau
University of Cambridge
Cambridge, UK
jcb82@cl.cam.ac.uk

Cormac Herley
Microsoft Research
Redmond, WA, USA
cormac@microsoft.com

Paul C. van Oorschot
Carleton University
Ottawa, ON, Canada
paulv@scs.carleton.ca

Frank Stajano[†]
University of Cambridge
Cambridge, UK
frank.stajano@cl.cam.ac.uk

http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-817.pdf



				Usability								Deployability						Security										
Category	Scheme	Described in section	Reference	*Memorywise-Effortless*	*Scalable-for-Users*	*Nothing-to-Carry*	*Physically-Effortless*	*Easy-to-Learn*	*Efficient-to-Use*	*Infrequent-Errors*	*Easy-Recovery-from-Loss*	*Accessible*	*Negligible-Cost-per-User*	*Server-Compatible*	*Browser-Compatible*	*Mature*	*Non-Proprietary*	*Resilient-to-Physical-Observation*	*Resilient-to-Targeted-Impersonation*	*Resilient-to-Throttled-Guessing*	*Resilient-to-Unthrottled-Guessing*	*Resilient-to-Internal-Observation*	*Resilient-to-Leaks-from-Other-Verifiers*	*Resilient-to-Phishing*	*Resilient-to-Theft*	*No-Trusted-Third-Party*	*Requiring-Explicit-Consent*	*Unlinkable*
(Incumbent)	Web passwords	III	[13]			●		●	●	○	●	●	●	●	●	●	●		○						●	●	●	●
Password managers	Firefox	IV-A	[22]	○🟩	●🟩	○🟥	○🟩	●	●	●🟩	🟥	●	●	●	🟥	●	●	○🟩	○					●🟩	●	●	●	●
	LastPass		[42]	○🟩	●🟩	○🟥	○🟩	●	●	●🟩	○🟥	●	○🟥	●	🟥	●	🟥	○🟩	○	○🟩	○🟩		○🟩	●🟩	●	🟥	●	●
Proxy	URRSA	IV-B	[5]	●🟩		🟥		●	🟥	○	🟥	🟥	●	○🟥	●	🟥	🟥		○			○🟩		●🟩	🟥	🟥	●	●
	Impostor		[23]	○🟩	●🟩	●		●	🟥	🟥	●	●	🟥	●	○🟥	🟥	●	●🟩	○			○🟩		●🟩	●	🟥	🟥	●
Federated	OpenID	IV-C	[27]	○🟩	●🟩	●	○🟩	○🟥	●	●🟩	●	●	●	🟥	●	●	●	○🟩	○	○🟩	○🟩		●🟩		●	🟥	●	🟥
	Microsoft Passport		[43]	○🟩	●🟩	●	○🟩	●	●	●🟩	●	●	🟥	🟥	●	●	🟥	○🟩	○	○🟩	○🟩		●🟩		●	🟥	●	🟥
	Facebook Connect		[44]	○🟩	●🟩	●	○🟩	●	●	●🟩	●	●	●	🟥	●	●	🟥	○🟩	○	○🟩	○🟩		●🟩		●	🟥	🟥	🟥
	BrowserID		[45]	○🟩	●🟩	●	○🟩	●	●	●🟩	●	●	●	🟥	○🟥	○🟥	●	○🟩	○	○🟩	○🟩		●🟩		●	🟥	●	🟥
	OTP over email		[46]	○🟩	●🟩	●		●	🟥	●🟩	●	●	●	🟥	●	🟥	●	○🟩	○	○🟩	○🟩		●🟩	●🟩	●	🟥	●	🟥
Graphical	PCCP	IV-D	[7]			●		●	○🟥	○	●	🟥	●	🟥	●	🟥	●		●🟩	○🟩			●🟩	●🟩	●	●	●	●
	PassGo		[47]			●		●	○🟥	○	●	🟥	●	🟥	●	○🟥	●		●🟩						●	●	●	●
Cognitive	GrIDsure (original)	IV-E	[30]			●		●	○🟥	○	●	🟥	●	🟥	●	🟥	🟥		●🟩						●	●	●	●
	Weinshall		[48]			●		🟥	🟥	🟥	🟥	🟥	●	🟥	●	🟥	●	○🟩	●🟩				●🟩	●🟩	●	●	●	●
	Hopper Blum		[49]			●		🟥	🟥	🟥	🟥	●	●	🟥	●	🟥	●	○🟩	●🟩				●🟩	●🟩	●	●	●	●
	Word Association		[50]			●		●	●	○	○🟥	●	●	🟥	●	🟥	●		🟥						●	●	●	●
Paper tokens	OTPW	IV-F	[33]			🟥		●	🟥	🟥	●	🟥	●	🟥	●	●	●		●🟩	●🟩	●🟩	●🟩	●🟩	●🟩	●	●	●	●
	S/KEY		[32]	●🟩		🟥		●	🟥	○	●	🟥	●	🟥	●	●	●		●🟩	●🟩	●🟩	●🟩	●🟩	○🟩	🟥	●	●	●
	PIN+TAN		[51]			🟥		●	🟥	○	○🟥	🟥	○🟥	🟥	●	●	●		●🟩	●🟩	●🟩	●🟩	●🟩	●🟩	○🟥	●	●	●
Visual crypto	PassWindow		[52]	●🟩		🟥		🟥	🟥	🟥	🟥	🟥	○🟥	🟥	●	●	🟥	○🟩	●🟩	●🟩	●🟩	●🟩	●🟩	●🟩	🟥	●	●	●
Hardware tokens	RSA SecurID	IV-G	[34]			🟥		●	○🟥	○	🟥	🟥	🟥	🟥	●	●	🟥	●🟩	●🟩	●🟩	●🟩	●🟩	●🟩	●🟩	●	🟥	●	●
	Yubikey		[53]			🟥		●	○🟥	○	🟥	●	🟥	🟥	●	●	🟥	●🟩	●🟩	●🟩	●🟩	●🟩	●🟩	●🟩	●	🟥	●	●
	Ironkey		[54]	○🟩	●🟩	🟥	○🟩	○🟥	○🟥	○	🟥	●	🟥	●	●	●	🟥	●🟩	○			○🟩		●🟩	●	●	●	●
	CAP reader		[55]			🟥		●	○🟥	○	🟥	🟥	🟥	🟥	●	●	🟥	●🟩	●🟩	●🟩	●🟩	●🟩	●🟩	●🟩	●	●	●	●
	Pico		[8]	●🟩	●🟩	🟥	●🟩	🟥	○🟥	○	🟥	🟥	🟥	🟥	🟥	🟥	●	●🟩	●🟩	●🟩	●🟩	●🟩	●🟩	●🟩	○🟥	●	●	●
Phone-based	Phoolproof	IV-H	[36]			○🟥		●	○🟥	○	🟥	○🟥	○🟥	○🟥	🟥	🟥	●	●🟩	●🟩	●🟩	●🟩	○🟩	●🟩	●🟩	●	●	●	●
	Cronto		[56]			○🟥		●	○🟥	○	🟥	🟥	○🟥	🟥	●	●	🟥	●🟩	●🟩	●🟩	●🟩	○🟩	●🟩	●🟩	●	●	●	●
	MP-Auth		[6]			○🟥		●	○🟥	🟥	○🟥	○🟥	○🟥	🟥	🟥	🟥	●		○					●🟩	●	●	●	●
	OTP over SMS			●🟩	●🟩	○🟥		●	🟥	○	○🟥	○🟥	🟥	🟥	●	●	●	●🟩	●🟩	●🟩	●🟩	○🟩	●🟩	●🟩	○🟥	🟥	●	●
	Google 2-Step		[57]			○🟥		●	○🟥	○	○🟥	○🟥	🟥	🟥	●	●	🟥	○🟩	○	●🟩	●🟩		●🟩	●🟩	●	●	●	●
Biometric	Fingerprint	IV-I	[38]	●🟩	●🟩	●	○🟩	●	○🟥	🟥	🟥	○🟥	🟥	🟥	🟥	○🟥	🟥	●🟩	🟥	●🟩					🟥	●	●	🟥
	Iris		[39]	●🟩	●🟩	●	○🟩	●	○🟥	🟥	🟥	○🟥	🟥	🟥	🟥	○🟥	🟥	●🟩	🟥	●🟩					🟥	●	○🟥	🟥
	Voice		[40]	●🟩	●🟩	●	○🟩	●	○🟥	🟥	🟥	○🟥	○🟥	🟥	○🟥	○🟥	🟥	●🟩	🟥	○🟩					🟥	●	●	🟥
Recovery	Personal knowledge		[58]	○🟩		●		●	●	○	●	●	●	🟥	●	●	●		🟥						●	●	●	●
	Preference-based		[59]	○🟩		●		●	○🟥	●🟩	○🟥	●	●	🟥	●	🟥	🟥		○					●🟩	●	●	●	●
	Social re-auth.		[60]			●		●	🟥	●🟩	🟥	●	●	🟥	●	○🟥	🟥	○🟩	🟥	●🟩	●🟩	○🟩	○🟩	●🟩	●	🟥	●	○🟥

●= offers the benefit; ○= almost offers the benefit; *no circle* = does not offer the benefit.
🟩= better than passwords; 🟥= worse than passwords; *no background pattern* = no change.