

# 2550 Intro to cybersecurity

## L18: Social Engineering

abhi shelat

Thanks Christo & Steve  
Myers for slides!

# Failures of Operation

Social engineering

# Baiting

Very simple physical attack

1. Preload USB keys with malware
2. Drop the keys in public, near victims
3. Wait for victims to pick up and plug in
4. Victim executes malware
  - Either by accident due to curiosity
  - Or autorun by the OS (e.g. Windows)



# Baiting

Mr. Robot FTW ;)

Very simple physical attack

1. Preload USB keys with malware
2. Drop the keys in public, near victims
3. Wait for victims to pick up and plug in
4. Victim executes malware
  - Either by accident due to curiosity
  - Or autorun by the OS (e.g. Windows)





# Tailgating

Technique used by penetration testers

Goal: break in to a secure facility

- Security guards at the main entrance
- All doors have keycard access control

Idea:

1. Wait for an unsuspecting employee to open a door
2. Follow them inside
3. Leverages courtesy bias and ingroup bias





# Phishing

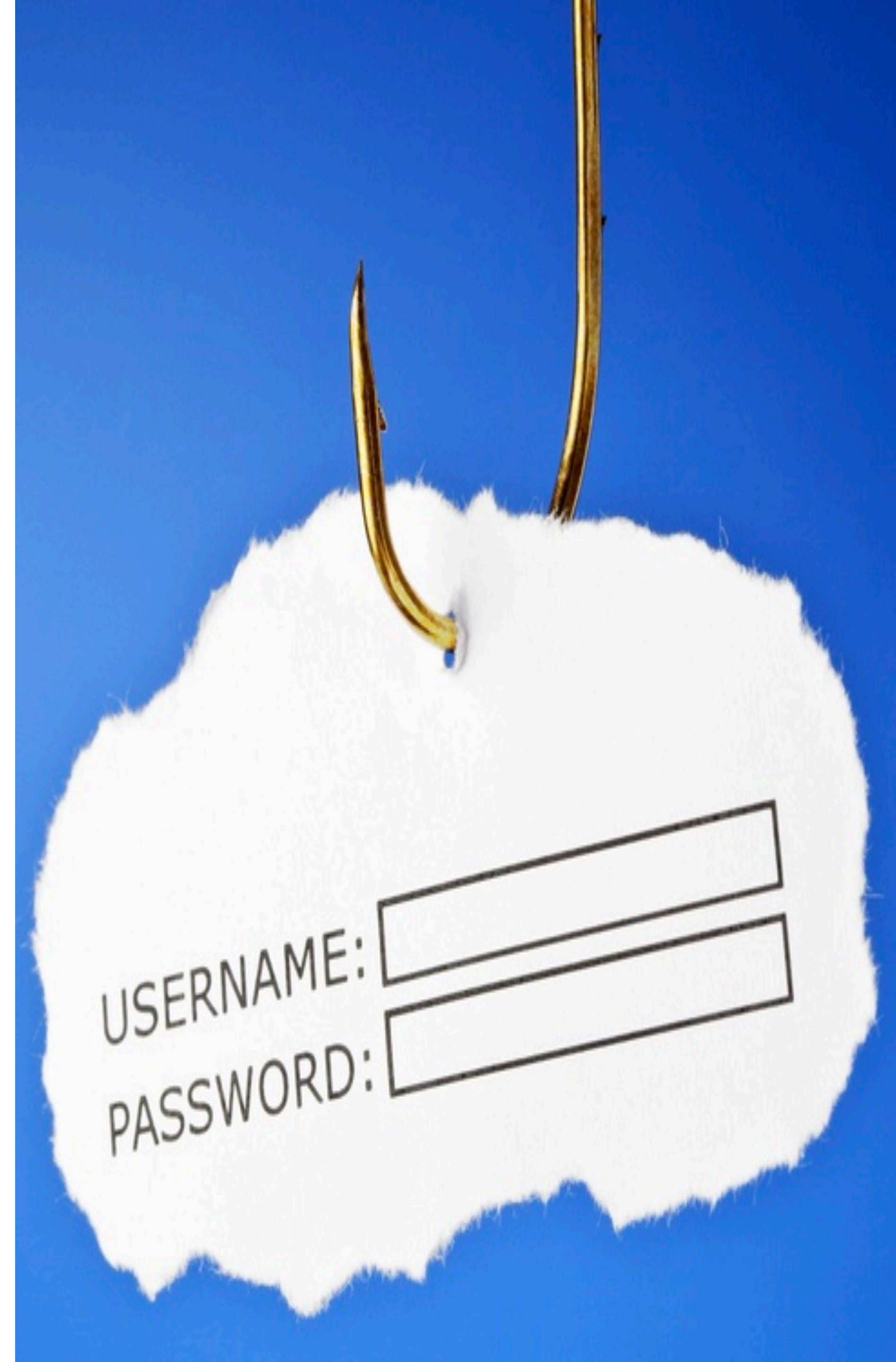
Attempts to coerce sensitive info from targets

Spread via email, SMS, messaging apps

- Careful framing
  - Banks, social networks, webmail
- Leverages urgency
  - “You will lose access to your account!”

Trick the victim into visiting a carefully constructed landing page

- User inputs sensitive info
- Passwords, social security numbers, credit cards, bank accounts, etc.



# John Podesta Phishing Email

- Sent by Russian intelligence to Clinton campaign staffers
- Podesta (campaign manager) asked IT if the mail was legit
- IT erroneously responded “this is a legitimate email”
- Account compromised, emails dumped to Wikileaks
- Massive political scandal

```
> *From:* Google <no-reply@accounts.googlemail.com>
> *Date:* March 19, 2016 at 4:34:30 AM EDT
> *To:* john.podesta@gmail.com
> *Subject:* *Someone has your password*
>
> Someone has your password
> Hi John
>
> Someone just used your password to try to sign in to your Google Account
> [REDACTED]@gmail.com.
>
> Details:
> Saturday, 19 March, 8:34:30 UTC
> IP Address: 134.249.139.239
> Location: Ukraine
>
> Google stopped this sign-in attempt. You should change your password
> immediately.
>
> CHANGE PASSWORD <https://bit.ly/1PibSU0>
>
> Best,
> The Gmail Team
> You received this mandatory email service announcement to update you about
> important changes to your Google product or account.
```



# John Podesta Phishing Email

- Sent by Russian intelligence to Clinton campaign staffers
- Podesta (campaign manager) asked IT if the mail was legit
- IT erroneously responded “this is a legitimate email”
- Account compromised, emails dumped to Wikileaks
- Massive political scandal

```
> *From:* Google <no-reply@accounts.googlemail.com>
```

```
> Date: March 19, 2016 at 4:34:30 AM EDT
```

```
> *To:* john.podesta@gmail.com
```

```
> *Subject:* *Someone has your password*
```

```
>
```

```
> Someone has your password
```

```
> Hi John
```

```
>
```

```
> Someone just used your password to try to sign in to your Google Account
```

```
> [REDACTED]@gmail.com.
```

```
>
```

```
> Details:
```

```
> Saturday, 19 March, 8:34:30 UTC
```

```
> IP Address: 134.249.139.239
```

```
> Location: Ukraine
```

```
>
```

```
> Google stopped this sign-in attempt. You should change your password
```

```
> immediately.
```

```
>
```

```
> CHANGE PASSWORD <https://bit.ly/1PibSU0>
```

```
>
```

```
> Best,
```

```
> The Gmail Team
```

```
> You received this mandatory email service announcement to update you about
```

```
> important changes to your Google product or account.
```

```
>
```

# John Podesta Phishing Email

- Sent by Russian intelligence to Clinton campaign staffers
- Podesta (campaign manager) asked IT if the mail was legit
- IT erroneously responded “this is a legitimate email”
- Account compromised, emails dumped to Wikileaks
- Massive political scandal

```
> *From:* Google <no-reply@accounts.googlemail.com>
```

```
> Date: March 19, 2016 at 4:34:30 AM EDT
```

```
> *To:* john.podesta@gmail.com
```

```
> *Subject:* *Someone has your password*
```

```
>
```

```
> Someone has your password
```

```
> Hi John
```

```
> Someone just used your password to try to sign in to your Google Account
```

```
> [REDACTED]@gmail.com.
```

```
>
```

```
> Details:
```

```
> Saturday, 19 March, 8:34:30 UTC
```

```
> IP Address: 134.249.139.239
```

```
> Location: Ukraine
```

```
>
```

```
> Google stopped this sign-in attempt. You should change your password
```

```
> immediately.
```

```
>
```

```
> CHANGE PASSWORD <https://bit.ly/1PibSU0>
```

```
>
```

```
> Best,
```

```
> The Gmail Team
```

```
> You received this mandatory email service announcement to update you about
```

```
> important changes to your Google product or account.
```

```
>
```



# John Podesta Phishing Email

- Sent by Russian intelligence to Clinton campaign staffers
- Podesta (campaign manager) asked IT if the mail was legit
- IT erroneously responded “this is a legitimate email”
- Account compromised, emails dumped to Wikileaks
- Massive political scandal

```
> *From:* Google <no-reply@accounts.googlemail.com>
```

```
> Date: March 19, 2016 at 4:34:30 AM EDT
```

```
> *To:* john.podesta@gmail.com
```

```
> *Subject:* *Someone has your password*
```

```
>
```

```
> Someone has your password
```

```
> Hi John
```

```
> Someone just used your password to try to sign in to your Google Account
```

```
> [REDACTED]@gmail.com.
```

```
>
```

```
> Details:
```

```
> Saturday, 19 March, 8:34:30 UTC
```

```
> IP Address: 134.249.139.239
```

```
> Location: Ukraine
```

```
>
```

```
> Google stopped this sign-in attempt. You should change your password
```

```
> immediately.
```

```
>
```

```
> CHANGE PASSWORD <https://bit.ly/1PibSU0>
```

```
>
```

```
> Best,
```

```
> The Gmail Team
```

```
> You received this mandatory email service announcement to update you about
```

```
> important changes to your Google product or account.
```

```
>
```

# John Podesta Phishing Email

- Sent by Russian intelligence to Clinton campaign staffers
- Podesta (campaign manager) asked IT if the mail was legit
- IT erroneously responded “this is a legitimate email”
- Account compromised, emails dumped to Wikileaks
- Massive political scandal

```
> *From:* Google <no-reply@accounts.googlemail.com>
```

```
> Date: March 19, 2016 at 4:34:30 AM EDT
```

```
> *To:* john.podesta@gmail.com
```

```
> *Subject:* *Someone has your password*
```

```
>
```

```
> Someone has your password
```

```
> Hi John
```

```
> Someone just used your password to try to sign in to your Google Account
```

```
> [REDACTED]@gmail.com.
```

```
>
```

```
> Details:
```

```
> Saturday, 19 March, 8:34:30 UTC
```

```
> IP Address: 134.249.139.239
```

```
> Location: Ukraine
```

```
>
```

```
> Google stopped this sign-in attempt. You should change your password
```

```
> immediately.
```

```
>
```

```
> CHANGE PASSWORD <https://bit.ly/1PibSU0>
```

```
>
```

```
> Best,
```

```
> The Gmail Team
```

```
> You received this mandatory email service announcement to update you about
```

```
> important changes to your Google product or account.
```

```
>
```





Online Banking

Learn More | Enroll Online eTimeBanker® Sign In:

User Name: Password:

SIGN IN

Forgot Password?

Other Online Services:

Select... GO



HOME EQUITY

Get in on the Great Rate Lock-in! Click here for the key

Locations

State: All

ZIP code:

LOCATE

CONSUMER ALERT!

Tips on protecting yourself and how to report suspicious activities

READ MORE

News Bulletin

June 14, 2005 | BancWest

Personal Banking

Welcome to your community bank.

First job. Last job. New home. College tuition. We're here to help guide your finances through the challenges of every life stage.

- Checking Savings & CDs Debit & Credit Cards Online Banking Wealth & Trust Consumer Loans Private Banking More ...

Tennis. Beach Games. Rodeo.

Join us for summer fun this week only!



Small Business Banking

Taking care of business. Across town. Around the globe.

As you navigate your business through all its cycles, you're not on your own. We assign a dedicated relationship manager to help you make the right financial choices.

- Business Checking Cash Management Merchant Services Loans & Lines SBA Lending More...

Commercial Banking

Your cornerstone of stability and growth. Middle-market to multi-national, our corporate



# Spear Phishing

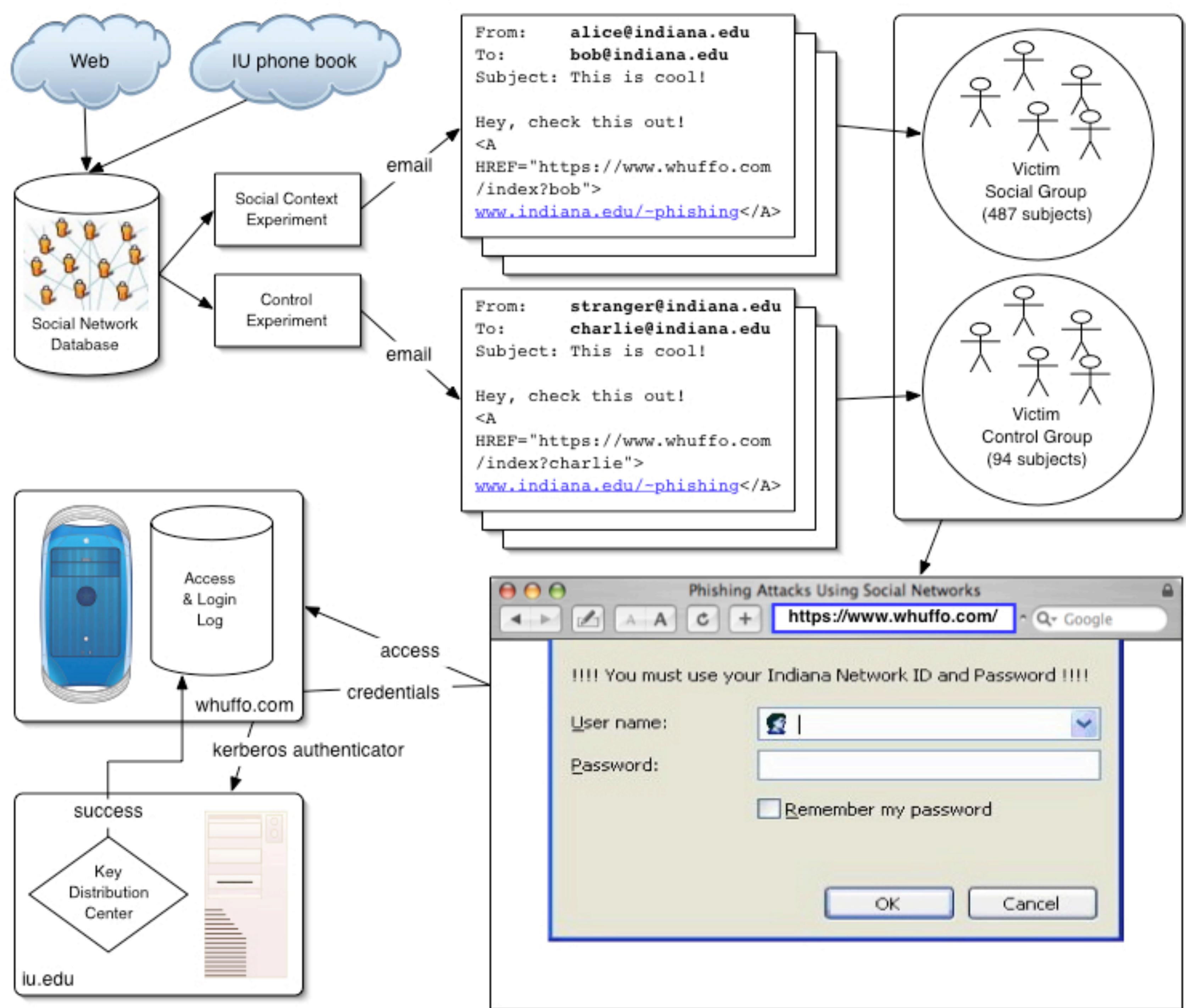
Advanced form of phishing

Highly targeted emails sent to high-value victims

- Includes many details about the target
- Does not trigger spam filters

Very challenging to detect by people and anomaly detectors

- May be sent from hacked, legit email accounts
- Or may use crafted domain names
  - E.g. googlemail.com





# VOIP Phishing

**Lure:** Get victim to call a bogus 800... number about their account.

**Hook:** Have the human on the other end extract the victim's information.

From: FlagStar Bank <[usflag60536@flagstar.com](mailto:usflag60536@flagstar.com)>

Date: 11 Sep 2007 10:55:21 -0400

To: <[samyers@indiana.edu](mailto:samyers@indiana.edu)>

Subject: You have one new private message

Dear FlagStar Bank card holder,

You have one new private message.

Please call free 800-870-8124 to listen to your private message.

Copyright ©2007 FlagStar Bank

**Source: Steven Myers, IU**

From: FlagStar Bank <[usflag60536@flagstar.com](mailto:usflag60536@flagstar.com)>

Date: 11 Sep 2007 10:55:21 -0400

To: <[samyers@indiana.edu](mailto:samyers@indiana.edu)>

Subject: You have one new private message

Dear FlagStar Bank card holder,

You have one new private message.

Please call free 800-870-8124 to listen to your private message.

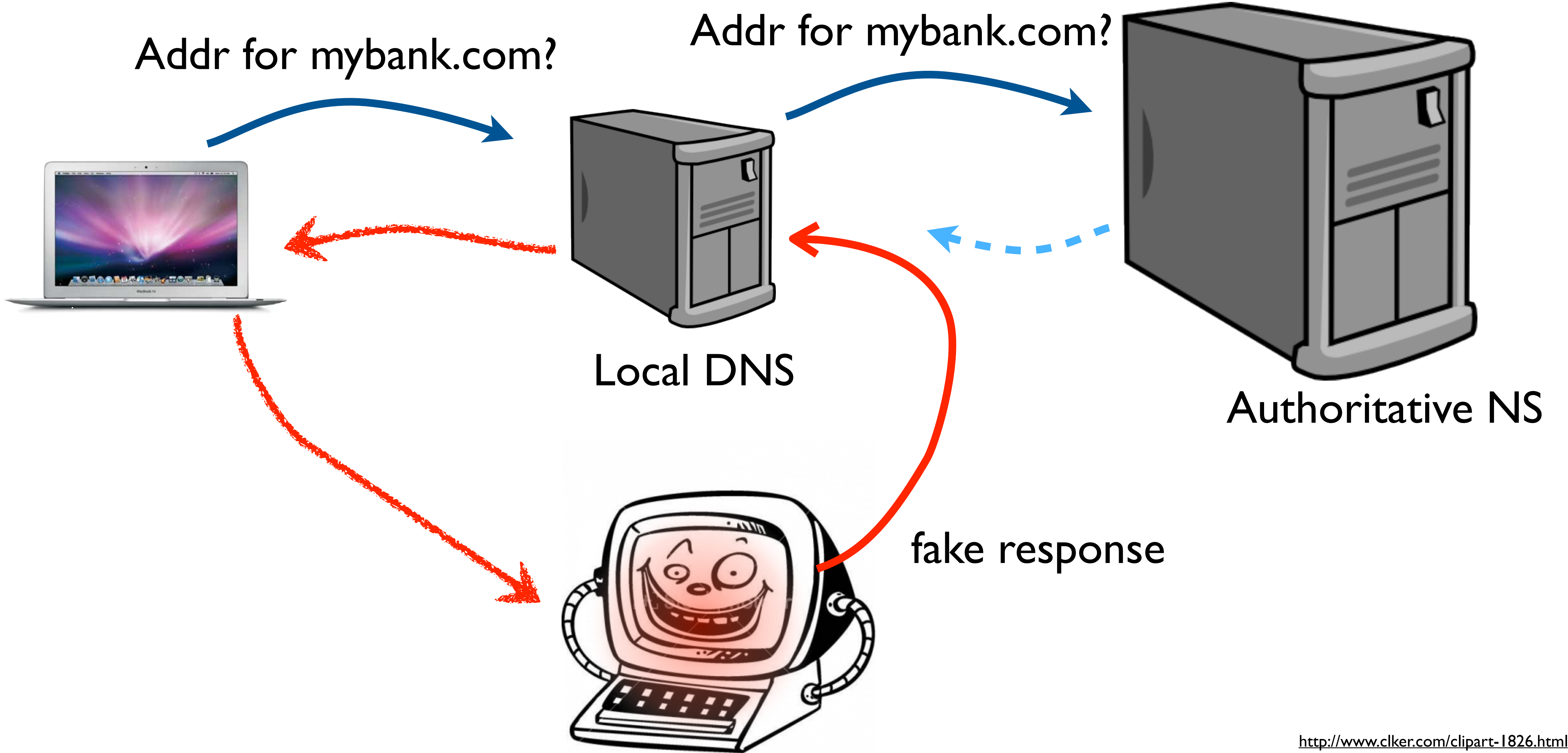
Copyright ©2007 FlagStar Bank

**Source: Steven Myers, IU**

# DNS Attack + Phishing = Pharming

**Lure:** Attack victim's DNS in order to convince them to navigate to a bogus site.

**Hook:** A website designed to mimic legitimate site and collect confidential information.





# CEO Fraud

Specific type of spear phishing

Targets employees with access to corporate bank accounts

- Attacker impersonates the company CEO
- Asks that money be wired to the attacker's bank account

# CEO Fraud

Specific type of spear phishing

Targets employees with access to corporate bank accounts

- Attacker impersonates the company CEO
- Asks that money be wired to the attacker's bank account

Exploits many cognitive biases

- Context and framing – Uses real names, jargon, and writing style
- Authority bias – orders from the CEO
- Creates a sense of urgency – “payment is late, send right away”

# CEO Fraud

Specific type of spear phishing

Targets employees with access to corporate bank accounts

- Attacker impersonates the company CEO
- Asks that money be wired to the attacker's bank account

Exploits many cognitive biases

- Context and framing – Uses real names, jargon, and writing style
- Authority bias – orders from the CEO
- Creates a sense of urgency – “payment is late, send right away”

Attacker may follow-up with more emails or calls

- Further increases the sophistication of the attack

13 July 2016 at 9:38 AM



To: [REDACTED]

Reply-To: [REDACTED]

Payment

---

Hi Michael,

Please find enclosed vendor banking instructions for a payment that was suppose to go out in the previous week. I need you to process it immediately.

I am a bit busy now but will give you a call within the hour regarding the payment.

Regards,

[REDACTED]

Sent from my Mobile

**From:** "Gatterbauer, Wolfgang" <[w.gatterbauer@northeastern.edu](mailto:w.gatterbauer@northeastern.edu)>

**Date:** Saturday, November 10, 2018 at 9:17 PM

**To:** "Brodley, Carla" <[c.brodley@northeastern.edu](mailto:c.brodley@northeastern.edu)>, "[brodleycarla@gmail.com](mailto:brodleycarla@gmail.com)" <[brodleycarla@gmail.com](mailto:brodleycarla@gmail.com)>

**Subject:** Fwd: Are you on campus?

Hi Carla,

I just got this email below from an account claiming to be you.

In case it was really sent from you (which I doubt you won't spell "Clara") feel free to call me on my cell phone 206 913 8820.

Otherwise, I assume a number of other people may have received a similar email today, not sure for what purpose...

If you prefer, I could go back and forth with that email to find out (?)

Best wishes,  
---Wolfgang

Begin forwarded message:

**From:** "Carla E.Brodley" <[c.brodley1342@gmail.com](mailto:c.brodley1342@gmail.com)>

**Subject:** Are you on campus?

**Date:** November 10, 2018 at 8:07:46 PM EST

**To:** [wolfgang@ccis.neu.edu](mailto:wolfgang@ccis.neu.edu)

Available?

Clara E.Brodley  
Dean - College of Computer and Information Science.  
440 Huntington Avenue  
202C West Village H  
Boston, MA 02115



# Advance-fee Scams

Also known as Nigerian prince or 419 scams

- Known as the “Spanish prisoner” con in the 18<sup>th</sup> century

Attacker entices the victim with promise of huge financial reward

But, victim must pay a small fee up-front



## REQUEST FOR ASSISTANCE-STRICTLY CONFIDENTIAL

I am Dr. Bakare Tunde, the cousin of Nigerian Astronaut, Air Force Major Abacha Tunde. He was the first African in space when he made a secret flight to the Salyut 6 space station in 1979. He was on a later Soviet spaceflight, Soyuz T-16Z to the secret Soviet military space station Salyut 8T in 1989. He was stranded there in 1990 when the Soviet Union was dissolved. His other Soviet crew members returned to earth on the Soyuz T-16Z, but his place was taken up by return cargo. There have been occasional Progrez supply flights to keep him going since that time. He is in good humor, but wants to come home.

In the 14-years since he has been on the station, he has accumulated flight pay and interest amounting to almost \$ 15,000,000 American Dollars. This is held in a trust at the Lagos National Savings and Trust Association. If we can obtain access to this money, we can place a down payment with the Russian Space Authorities for a Soyuz return flight to bring him back to Earth. I am told this will cost \$ 3,000,000 American Dollars. In order to access the his trust fund we need your assistance.

Consequently, my colleagues and I are willing to transfer the total amount to your account or subsequent disbursement, since we as civil servants are prohibited by the Code of Conduct Bureau (Civil Service Laws) from opening and/ or operating foreign accounts in our names.

Needless to say, the trust reposed on you at this juncture is enormous. In return, we have agreed to offer you 20 percent of the transferred sum...

# Scareware

Attempts to convince the victim to install malware on their system

Paradoxically, leverages people's fears of security problems

- Virus and malware infections
- Data breaches

Distributed via online ads and compromised websites



# Scareware

Attempts to convince the victim to install malware on their system

Paradoxically, leverages people's fears of security problems

- Virus and malware infections
- Data breaches

Distributed via online ads and compromised websites

Whole fake antivirus industry around these scams

- More on this when you read *Spam Nation*
- Scareware companies have real customer support hotlines
- Sometimes the products actually remove malware
  - But only from competing crime gangs ;)



Microsoft Security Essentials

# WINDOWS VIRUS WARNING!





Identity Theft and Hacking Possibilities.

Contact emergency virus support now.


## 0-800-051-3723

The system have found (4) viruses that



Threat	Alert
	Trojan.FakeAV-Download
	Spyware.BANKER.ID
	Trojan.FakeAV-Download
	Trojan.FakeAV-Download

Message from webpage

 Microsoft Detected Security Error, Due to Suspicious Activity Found On Your Computer. Contact Microsoft Certified Live Technicians 0-800-051-3723 (Toll Free)

OK

 Your personal and financial information is compromised call **0-800-051-3723** to be secured.

Recommended:





Context and framing:  
real security logos  
and product names

The screenshot shows a web browser window with a URL starting with '247tech.help'. The page features the Microsoft Security Essentials logo and a large warning: 'WINDOWS VIRUS WARNING! Identity Theft and Hacking Possibilities. Contact emergency virus support now. 0-800-051-3723'. A system dialog box titled 'Message from webpage' is overlaid, displaying a warning icon and the text: 'Microsoft Detected Security Error, Due to Suspicious Activity Found On Your Computer. Contact Microsoft Certified Live Technicians 0-800-051-3723 (Toll Free)'. Below the dialog, a table lists detected threats, and a footer contains a warning icon and the text: 'Your personal and financial information is compromised call 0-800-051-3723 to be secured.' The Microsoft logo is visible in the bottom right corner.

247tech.help/crt/uk\_seg1003/micr\_ess

Microsoft Security Essentials

# WINDOWS VIRUS WARNING!

Identity Theft and Hacking Possibilities.  
Contact emergency virus support now.

## 0-800-051-3723

The system have found (4) viruses that

Threat	Alert
	Trojan.FakeAV-Download
	Spyware.BANKER.ID
	Trojan.FakeAV-Download
	Trojan.FakeAV-Download

Message from webpage

Microsoft Detected Security Error, Due to Suspicious Activity Found On Your Computer. Contact Microsoft Certified Live Technicians 0-800-051-3723 (Toll Free)

OK

Your personal and financial information is compromised call **0-800-051-3723** to be secured.

Recommended:

Microsoft



Context and framing:  
real security logos  
and product names

Urgency: you  
are infected!

The screenshot shows a web browser window with a URL starting with '247tech.help/crt/uk\_seg1003/micr\_ess'. The page features the Microsoft Security Essentials logo and a large warning: 'WINDOWS VIRUS WARNING! Identity Theft and Hacking Possibilities. Contact emergency virus support now. 0-800-051-3723'. Below this, a table lists detected threats, and a dialog box titled 'Message from webpage' displays a warning about suspicious activity and the same phone number. At the bottom, a footer states 'Your personal and financial information is compromised call 0-800-051-3723 to be secured.' and includes the Microsoft logo.

Threat	Alert
	Trojan.FakeAV-Download
	Spyware.BANKER.ID
	Trojan.FakeAV-Download
	Trojan.FakeAV-Download

Message from webpage

Microsoft Detected Security Error, Due to Suspicious Activity Found On Your Computer. Contact Microsoft Certified Live Technicians 0-800-051-3723 (Toll Free)

OK

Your personal and financial information is compromised call **0-800-051-3723** to be secured.

Recommended:



Context and framing:  
real security logos  
and product names

Urgency: you  
are infected!

Familiarity: real-  
looking security  
dialogs

The screenshot shows a web browser window with the address bar containing "247tech.help/crt/uk\_seg1003/micr\_ess". The page features the Microsoft Security Essentials logo and a large warning: "WINDOWS VIRUS WARNING! Identity Theft and Hacking Possibilities. Contact emergency virus support now. 0-800-051-3723". A "Message from webpage" dialog box is overlaid, displaying a warning icon and the text: "Microsoft Detected Security Error, Due to Suspicious Activity Found On Your Computer. Contact Microsoft Certified Live Technicians 0-800-051-3723 (Toll Free)". Below the dialog, a table lists detected threats:

Threat	Alert
	Trojan.FakeAV-Download
	Spyware.BANKER.ID
	Trojan.FakeAV-Download
	Trojan.FakeAV-Download

At the bottom of the page, a warning icon is followed by the text: "Your personal and financial information is compromised call 0-800-051-3723 to be secured." The Microsoft logo is visible in the bottom right corner.

# Sextortion

Relies on three generalizations:

1. People view porn on the internet
2. People assume their porn viewing habits are private
3. People reuse the same password across multiple services

Leverages several cognitive biases

- Urgency – “pay the ransom in 24 hours or else!”
- Fear of privacy and intimacy violations
- Belief bias – they have a password from one service, they must have it for all services



## Your Secret Life



Fri 9/28, 4:22 AM



Reply all | v

Hello!

I'm a member of an international hacker group.

As you could probably have guessed, your account [redacted] was hacked, because I sent message you from it.

Now I have access to you accounts!

For example, your password for [redacted] is [redacted]

Within a period from July 7, 2018 to September 23, 2018, you were infected by the virus we've created, through an adult website you've visited.

So far, we have access to your messages, social media accounts, and messengers.

Moreover, we've gotten full dumps of these data.

We are aware of your little and big secrets...yeah, you do have them. We saw and recorded your doings on porn websites. Your tastes are so weird, you know..

But the key thing is that sometimes we recorded you with your webcam, syncing the recordings with what you watched!

I think you are not interested show this video to your friends, relatives, and your intimate one...

Transfer \$700 to our Bitcoin wallet: 1Lughwk11SAsz54wZJ3bpGbNqGfVanMWzk

If you don't know about Bitcoin please input in Google "buy BTC". It's really easy.

I guarantee that after that, we'll erase all your "data" :D

A timer will start once you read this message. You have 48 hours to pay the above-mentioned amount.

Your data will be erased once the money are transferred.

If they are not, all your messages and videos recorded will be automatically sent to all your contacts found on your devices at the moment of infection.

You should always think about your security. We hope this case will teach you to keep secrets.

Take care of yourself.





## Your Secret Life



Fri, 9/28, 4:22 AM



Sent from "your email address" via spoofing





Reply all | v

Hello!

I'm a member of an international hacker group.

As you could probably have guessed, your account  was hacked, because I sent message you from it.

Now I have access to you accounts!

For example, your password for  is 

Within a period from July 7, 2018 to September 23, 2018, you were infected by the virus we've created, through an adult website you've visited. So far, we have access to your messages, social media accounts, and messengers. Moreover, we've gotten full dumps of these data.

We are aware of your little and big secrets...yeah, you do have them. We saw and recorded your doings on porn websites. Your tastes are so weird, you know..

But the key thing is that sometimes we recorded you with your webcam, syncing the recordings with what you watched! I think you are not interested show this video to your friends, relatives, and your intimate one...

Transfer \$700 to our Bitcoin wallet: 1Lughwk11SAsz54wZJ3bpGbNqGfVanMWzk  
If you don't know about Bitcoin please input in Google "buy BTC". It's really easy.

I guarantee that after that, we'll erase all your "data" :D

A timer will start once you read this message. You have 48 hours to pay the above-mentioned amount.

Your data will be erased once the money are transferred.

If they are not, all your messages and videos recorded will be automatically sent to all your contacts found on your devices at the moment of infection.

You should always think about your security. We hope this case will teach you to keep secrets.  
Take care of yourself.





## Your Secret Life



Sent from "your email address" via spoofing



Reply all | v

Fri 9/28, 4:22 AM





Hello!

I'm a member of an international hacker group.

As you could probably have guessed, your account  was hacked, because I sent message you from it.

Now I have access to you accounts!

For example, your password for  is 

Within a period from July 7, 2018 to September 23, 2018, you were infected by the virus we've created, through an adult website you've visited. So far, we have access to your messages, social media accounts, and messengers. Moreover, we've gotten full dumps of these data.

We are aware of your little and big secrets...yeah, you do have them. We saw and recorded your doings on porn websites. Your tastes are so weird, you know..

But the key thing is that sometimes we recorded you with your webcam, syncing the recordings with what you watched! I think you are not interested show this video to your friends, relatives, and your intimate one...

Transfer \$700 to our Bitcoin wallet: 1Lughwk11SAsz54wZJ3bpGbNqGfVanMWzk  
If you don't know about Bitcoin please input in Google "buy BTC". It's really easy.

I guarantee that after that, we'll erase all your "data" :D

A timer will start once you read this message. You have 48 hours to pay the above-mentioned amount.

Your data will be erased once the money are transferred.

If they are not, all your messages and videos recorded will be automatically sent to all your contacts found on your devices at the moment of infection.

You should always think about your security. We hope this case will teach you to keep secrets.

Take care of yourself.



Actual password taken from a pre-existing website breach



## Your Secret Life



Sent from "your email address" via spoofing



Reply all | v

Fri 9/28, 4:22 AM





Hello!

I'm a member of an international hacker group.

As you could probably have guessed, your account  was hacked, because I sent message you from it.

Now I have access to you accounts!

For example, your password for  is 

Within a period from July 7, 2018 to September 23, 2018, you were infected by the virus we've created, through an adult website you've visited. So far, we have access to your messages, social media accounts, and messengers. Moreover, we've gotten full dumps of these data.

We are aware of your little and big secrets...yeah, you do have them. We saw and recorded your doings on porn websites. Your tastes are so weird, you know..

But the key thing is that sometimes we recorded you with your webcam, syncing the recordings with what you watched! I think you are not interested show this video to your friends, relatives, and your intimate one...

Transfer \$700 to our Bitcoin wallet: 1Lughwk11SAsz54wZJ3bpGbNqGfVanMWzk  
If you don't know about Bitcoin please input in Google "buy BTC". It's really easy.

I guarantee that after that, we'll erase all your "data" :D

A timer will start once you read this message. You have 48 hours to pay the above-mentioned amount.

Your data will be erased once the money are transferred.

If they are not, all your messages and videos recorded will be automatically sent to all your contacts found on your devices at the moment of infection.

You should always think about your security. We hope this case will teach you to keep secrets.  
Take care of yourself.

Actual password taken from a pre-existing website breach



## Your Secret Life



Sent from "your email address" via spoofing



Reply all | v

Fri 9/28, 4:22 AM




Hello!

I'm a member of an international hacker group.

As you could probably have guessed, your account  was hacked, because I sent message you from it.

Now I have access to you accounts!

For example, your password for  is 

Within a period from July 7, 2018 to September 23, 2018, you were infected by the virus we've created, through an adult website you've visited. So far, we have access to your messages, social media accounts, and messengers. Moreover, we've gotten full dumps of these data.

We are aware of your little and big secrets...yeah, you do have them. We saw and recorded your doings on porn websites. Your tastes are so weird, you know..

But the key thing is that sometimes we recorded you with your webcam, syncing the recordings with what you watched! I think you are not interested show this video to your friends, relatives, and your intimate one...

Transfer \$700 to our Bitcoin wallet: 1Lughwk11SAsz54wZJ3bpGbNqGfVanMWzk  
If you don't know about Bitcoin please input in Google "buy BTC". It's really easy.

I guarantee that after that, we'll erase all your "data" :D

A timer will start once you read this message. You have 48 hours to pay the above-mentioned amount.

Your data will be erased once the money are transferred.

If they are not, all your messages and videos recorded will be automatically sent to all your contacts found on your devices at the moment of infection.

You should always think about your security. We hope this case will teach you to keep secrets.

Take care of yourself.



Actual password taken from a pre-existing website breach



## Your Secret Life



Fri 9/28, 4:22 AM



Sent from "your email address" via spoofing



Reply all | v



Actual password taken from a pre-existing website breach

Hello!

I'm a member of an international hacker group.

As you could probably have guessed, your account  was hacked, because I sent message you from it.

Now I have access to you accounts!

For example, your password for  is 

Within a period from July 7, 2018 to September 23, 2018, you were infected by the virus we've created, through an adult website you've visited. So far, we have access to your messages, social media accounts, and messengers. Moreover, we've gotten full dumps of these data.

We are aware of your little and big secrets...yeah, you do have them. We saw and recorded your doings on porn websites. Your tastes are so weird, you know..

But the key thing is that sometimes we recorded you with your webcam, syncing the recordings with what you watched! I think you are not interested show this video to your friends, relatives, and your intimate one...

Transfer \$700 to our Bitcoin wallet: 1Lughwk11SAsz54wZJ3bpGbNqGfVanMWzk  
If you don't know about Bitcoin please input in Google "buy BTC". It's really easy.

I guarantee that after that, we'll erase all your "data" :D

A timer will start once you read this message. You have 48 hours to pay the above-mentioned amount.

Your data will be erased once the money are transferred.

If they are not, all your messages and videos recorded will be automatically sent to all your contacts found on your devices at the moment of infection.

You should always think about your security. We hope this case will teach you to keep secrets.

Take care of yourself.





# Bespoke Attacks

- Attackers are constantly innovating new social engineering methods
- The Internet makes information easily accessible...
- ... and people easily reachable

It is tax season again and I just experienced an other level of frustration. This afternoon I received a call starting with:

- “Are you ———? You are a PhD student at Northeastern university? You are from China and started from 2011 and graduating this year, right?”

- “You are under a criminal investigation because you haven’t paid the education taxes (Form 8863).”

...

- “We know all your information and have been tracking you extensively for the last 2 months, because you are facing multiple charges.”

I was very suspicious of them and asked them how I could verify they were the real FBI. They said you can google the number and I saw this

Same number, pictures, addresses, etc. I was very convinced and panicked. They told me I have two options:

1) Pay the taxes today at IRS, or;

2) They will call the police to arrest me immediately

Definitely I choose option 1). Then they asked me to follow the exact procedure they told me: 1) stay on the phone, 2) do not talk to anyone about this because it is still a private case; 3) go to the authorized store (target, apple store, etc. ) to buy some vouchers to pay the IRS. It raised my suspicion again when they mentioned the voucher and the specific names of vouchers (I actually did take a cab to the Target on the boylston street because all the information looked so authentic), and asked them for verification again (my birthdate and SSN). They got furious, saying “OK, since your are not complying, we will call police to arrest you now.” Then my phone received an incoming call



About 205,000 results (0.62 seconds)

### Federal Bureau of Investigation in Lowell, MA - (978) 454-6972 - Buzzfile

[www.buzzfile.com/business/FBI-978-454-6972](http://www.buzzfile.com/business/FBI-978-454-6972)

Federal Bureau of Investigation, which also operates under the name FBI, is located in Lowell, Massachusetts. This organization primarily operates in the ...

### Federal Bureau of Investigation in Lowell, MA - (978) 454-6972 - Buzzfile

[www.buzzfile.com/business/Federal-Bureau-of-Investigation-978-454-6972](http://www.buzzfile.com/business/Federal-Bureau-of-Investigation-978-454-6972)

Federal Bureau of Investigation is located in Lowell, Massachusetts. This organization primarily operates in the General Government Administration business ...

### Boston – FBI

<https://www.fbi.gov/contact-us/field-offices/boston>

... days a week. You can also submit a tip electronically at [tips.fbi.gov](https://tips.fbi.gov). ... History of the FBI's Boston, Massachusetts Field Office. More ... Lowell, MA. Counties ...

### Federal Bureau-Investigation Lowell, MA 01851 - YP.com

[www.yellowpages.com](http://www.yellowpages.com) › Federal Government near Lowell, MA

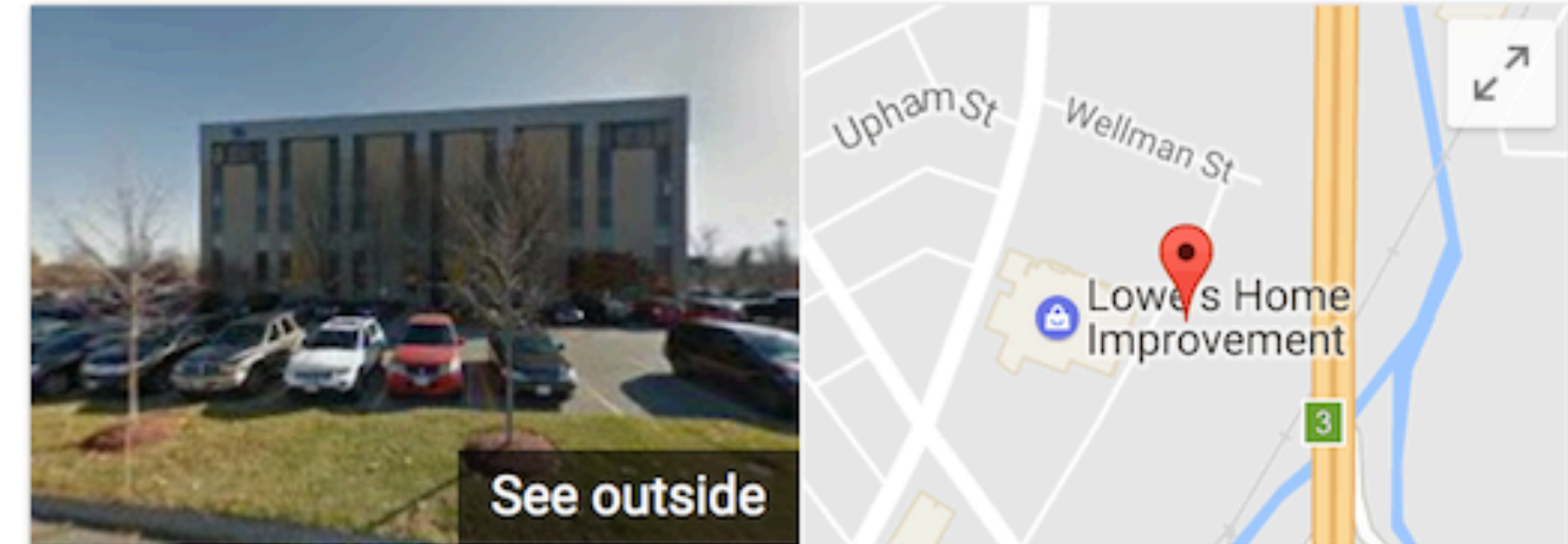
Get reviews, hours, directions, coupons and more for Federal Bureau-Investigation at 59 Lowes Way, Lowell, MA. Search for other Federal Government in Lowell ...

### Fbi in Lowell, Massachusetts with Reviews - YP.com

<https://www.yellowpages.com/lowell-ma/fbi>

Find 8 listings related to Fbi in Lowell on YP.com. See reviews, photos, directions, phone numbers and more for Fbi locations in Lowell, MA.

Federal Bureau Of Investigation Lowell MA 01851 - Manta.com



## Federal Bureau of Investigation

Website

Directions

Federal government office in Lowell, Massachusetts

**Address:** 59 Lowes Way # 201, Lowell, MA 01851

**Phone:** (978) 454-6972

[Suggest an edit](#) · [Own this business?](#)

Add missing information

[Add business hours](#)

Reviews

[Be the first to review](#)

Write a review

Add a photo

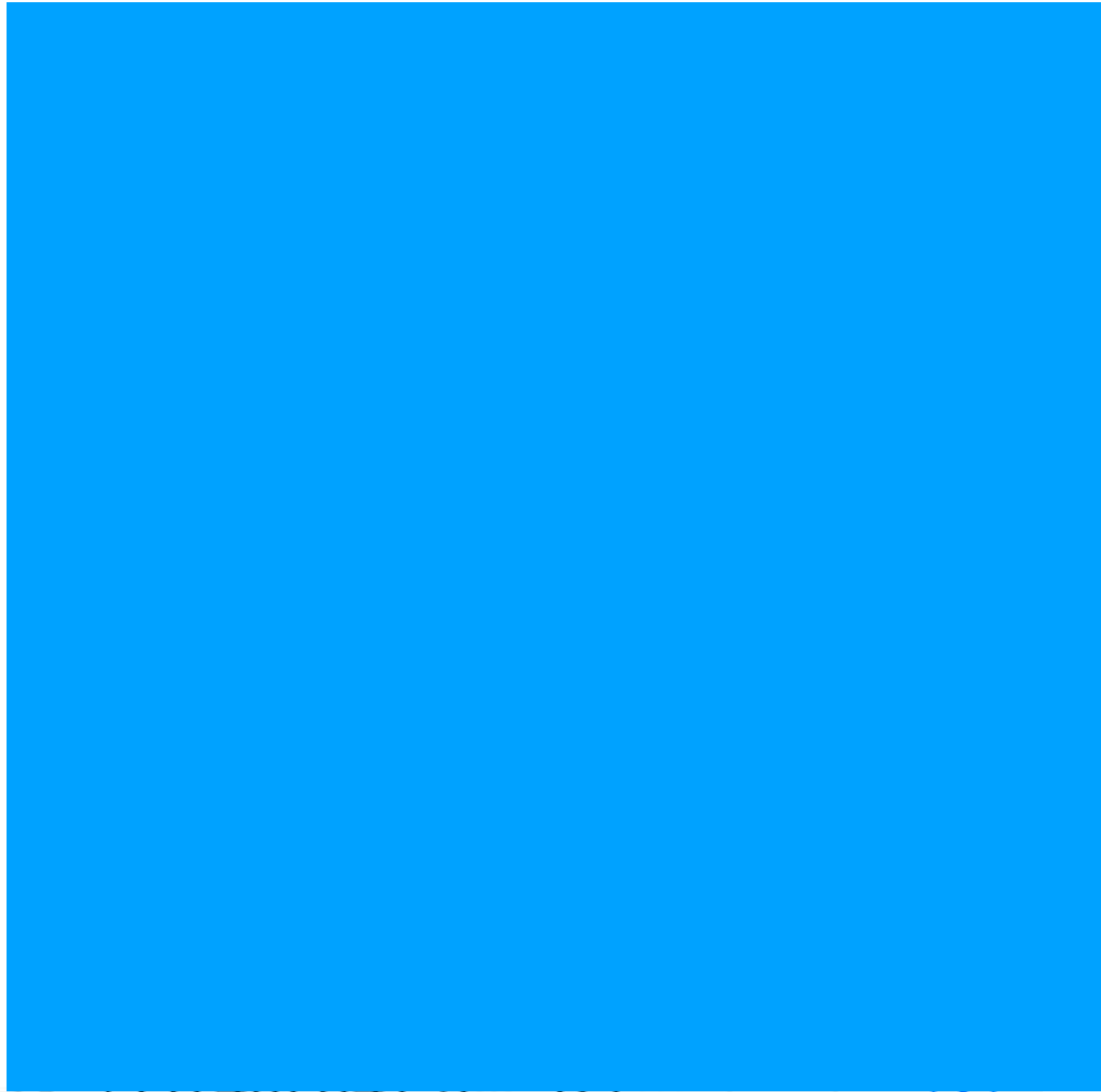
Feedback



All Missed Edit

+91 1 2:27 PM ⓘ  
India

(978) 454-6972 (2) 1:18 PM ⓘ  
Lowell, MA





Why so effective?

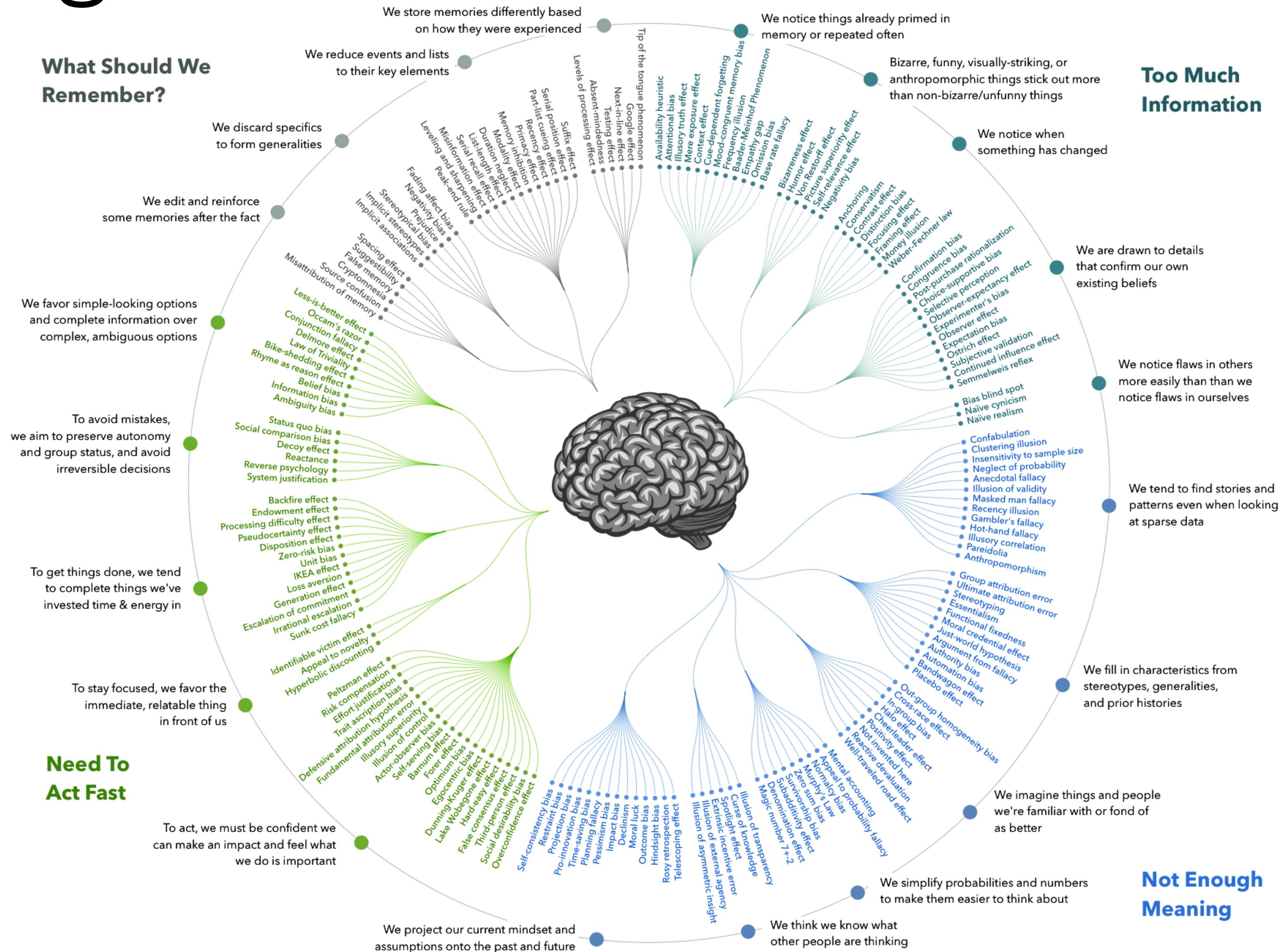


Humans rely on **heuristics** to handle **cognitive overload**





# Heuristics → Cognitive Bias



# Cognitive Biases

## Behavioral Biases

Belief bias

Confirmation bias

Courtesy bias

Framing effect

Stereotyping

## Social Biases

Authority bias

Halo effect

Ingroup bias

## Memory Biases

Context effect

Suggestibility



# Cognitive Biases

## Behavioral Biases

### Belief bias

- Evaluation of an argument is based on the believability of the conclusion

### Confirmation bias

- search out information that confirms existing preconceptions

### Courtesy bias

- Urge to avoid offending people

### Framing effect

- Drawing different conclusions from the same info, based on how it was presented

### Stereotyping

## Social Biases

### Authority bias

- Tendency to believe and be influenced by authority figures, regardless of content

### Halo effect

- Tendency for positive personality traits from one area to “spill” into another

### Ingroup bias

- Tendency to give preferential treatment to others from your own group

## Memory Biases

### Context effect

- Cognition and memory are dependent on context

### Suggestibility

- Misattributing ideas from the questioner as one's own

# Social Engineering Basics

Successful attacks rely on:

1. Information asymmetry
2. Context construction
3. Elicitation and persuasion

Cognitive biases are leveraged in all three steps





# Mitnick on Pretexting

“When you use social engineering, or ‘pretexting’, you become an actor playing a role... When you know the lingo and terminology, it established credibility—you’re legit, a coworker slogging in the trenches just like your targets, and they almost never question your authority... People in offices ordinarily give others the benefit of the doubt when the request appears to be authentic. People, as I learned at a very young age, are just too trusting.”

# Mitnick on Pretexting

Ingroup bias and stereotyping

Context and framing

Authority bias

“When you use social engineering, or pretexting, you become an actor playing a role... When you know the lingo and terminology, it establishes credibility—you’re legit, a coworker slogging in the trenches just like your targets, and they almost never question your authority... People in offices ordinarily give others the benefit of the doubt when the request appears to be authentic. People, as I learned at a very young age, are just too trusting.”

Suggestability

Courtesy bias



# Elicitation

Idea promoted by Christopher Hadnagy

- The ability to draw people out and make them trust you

Leveraging elicitation techniques

1. Be polite (courtesy bias)
2. Professionals want to appear well informed and intelligent
3. People are compelled to reciprocate praise
4. People respond kindly to concern
5. Most people don't routinely lie

# Persuasion

Ultimately, the goal is to make the victim take an action or reveal confidential information

## Psychological manipulation techniques

- Appeals to ego
- Making deliberate false statements
- Volunteering information (credibility bias)
- Assuming knowledge
- Effective use of questions (suggestibility)
- Quid pro quo: give something to get something in return

More effective when paired with cognitive biases

- Authority bias
- Belief bias
- Confirmation bias
- Ingroup bias



# Follow-through

Suddenly dropping the victim arouses suspicion

- Cutting off contact abruptly
- “Ghosting”

Provide logical follow-through

- Conversations should end normally
- Emails should be answered cordially
- Give the victim normal closure

# Kevin On Follow-through

“Chatting is the kind of extra little friendly touch that leaves people with a good feeling and makes after-the-fact suspicions that much less likely.”



Quote from [“Ghost in the Wires”](#) by Kevin Mitnick



# Case Study: Phishing

Evaluating emails

Evaluating websites

Does training work?

# Test

<https://www.phishingbox.com/phishing-test>





# John Podesta Phishing Email

```
> *From:* Google <no-reply@accounts.googlemail.com>
> *Date:* March 19, 2016 at 4:34:30 AM EDT
> *To:* john.podesta@gmail.com
> *Subject:* *Someone has your password*
>
> Someone has your password
> Hi John
>
> Someone just used your password to try to sign in to your Google Account
> [REDACTED]@gmail.com.
>
> Details:
> Saturday, 19 March, 8:34:30 UTC
> IP Address: 134.249.139.239
> Location: Ukraine
>
> Google stopped this sign-in attempt. You should change your password
> immediately.
>
> CHANGE PASSWORD <https://bit.ly/1PibSU0>
>
> Best,
> The Gmail Team
> You received this mandatory email service announcement to update you about
> important changes to your Google product or account.
```





Online Banking

Learn More | Enroll Online eTimeBanker® Sign In:

User Name: Password:

SIGN IN

Forgot Password?

Other Online Services:

Select... GO



Locations

State: All

ZIP code:

LOCATE

CONSUMER ALERT!

Tips on protecting yourself and how to report suspicious activities

READ MORE

News Bulletin

June 14, 2005 | BancWest

Personal Banking

Welcome to your community bank. First job. Last job. New home. College tuition. We're here to help guide your finances through the challenges of every life stage.

- Checking Savings & CDs Debit & Credit Cards Online Banking Wealth & Trust Consumer Loans Private Banking More ...

Tennis. Beach Games. Rodeo.

Join us for summer fun this week only!



Small Business Banking

Taking care of business. Across town. Around the globe. As you navigate your business through all its cycles, you're not on your own. We assign a dedicated relationship manager to help you make the right financial choices.

- Business Checking Cash Management Merchant Services Loans & Lines SBA Lending More...

Commercial Banking

Your cornerstone of stability and growth. Middle-market to multi-national, our corporate





“vv” instead of “w”

Online Banking

Learn More | Enroll Online eTimeBanker® Sign In:

User Name: Password:

SIGN IN

Forgot Password?

Other Online Services:

Select... GO



Locations

State: All

ZIP code:

LOCATE

CONSUMER ALERT! Tips on protecting yourself and how to report suspicious activities READ MORE

News Bulletin

June 14, 2005 | BancWest

Personal Banking

Welcome to your community bank. First job. Last job. New home. College tuition. We're here to help guide your finances through the challenges of every life stage. Stop by a branch to experience our hallmark service for yourself.

- Checking Savings & CDs Debit & Credit Cards Online Banking Wealth & Trust Consumer Loans Private Banking More ...

Tennis. Beach Games. Rodeo.

Join us for summer fun this week only!



Small Business Banking

Taking care of business. Across town. Around the globe.

As you navigate your business through all its cycles, you're not on your own. We assign a dedicated relationship manager to help you make the right financial choices. Give us a call. We pick up the phone!

- Business Checking Cash Management Merchant Services Loans & Lines SBA Lending More...

Commercial Banking

Your cornerstone of stability and growth. Middle-market to multi-national, our corporate



# Blackboard learn<sup>+</sup>

SCHOOL USER ID:

E-MAIL ADDRESS:

PASSWORD:

Login



Blackboard

© 1997-2013 Blackboard Inc. All Rights Reserved. U.S. Patent No. 7,493,396 and 7,558,853. Additional Patents Pending.

[Accessibility information](#) - [Installation details](#)



-----Original Message-----

From: Peggy Altman [<mailto:peggyaltman@usa.com>]

Sent: Tuesday, May 16, 2017 6:23 AM

To: You <[peggyaltman@usa.com](mailto:peggyaltman@usa.com)>

Subject: Charity Donation For You

Importance: High

Sensitivity: Personal

My name is Peggy Altman the personal assistant of Ms. Doris Buffett, a philanthropist and founder of a large private foundation. She is on a mission to give it all away while living; She always had the idea that wealth should be used to help each other which made her decide to give it all. Kindly acknowledge this message by replying and I will get back to you with more details.

Read more about her: <http://abcnews.go.com/GMA/Books/giving-dorris-buffett-story-michael-zitz/story?id=10827641>

Sincerely,

Peggy Altman.

# Why Do People Fall Prey to Phishing?

Evaluating the veracity of emails is challenging

- Non-spoofed header?
- Security indicators like DKIM and SPF?
- Personalization, e.g. your name?
- Quality of the text?



# Why Do People Fall Prey to Phishing?

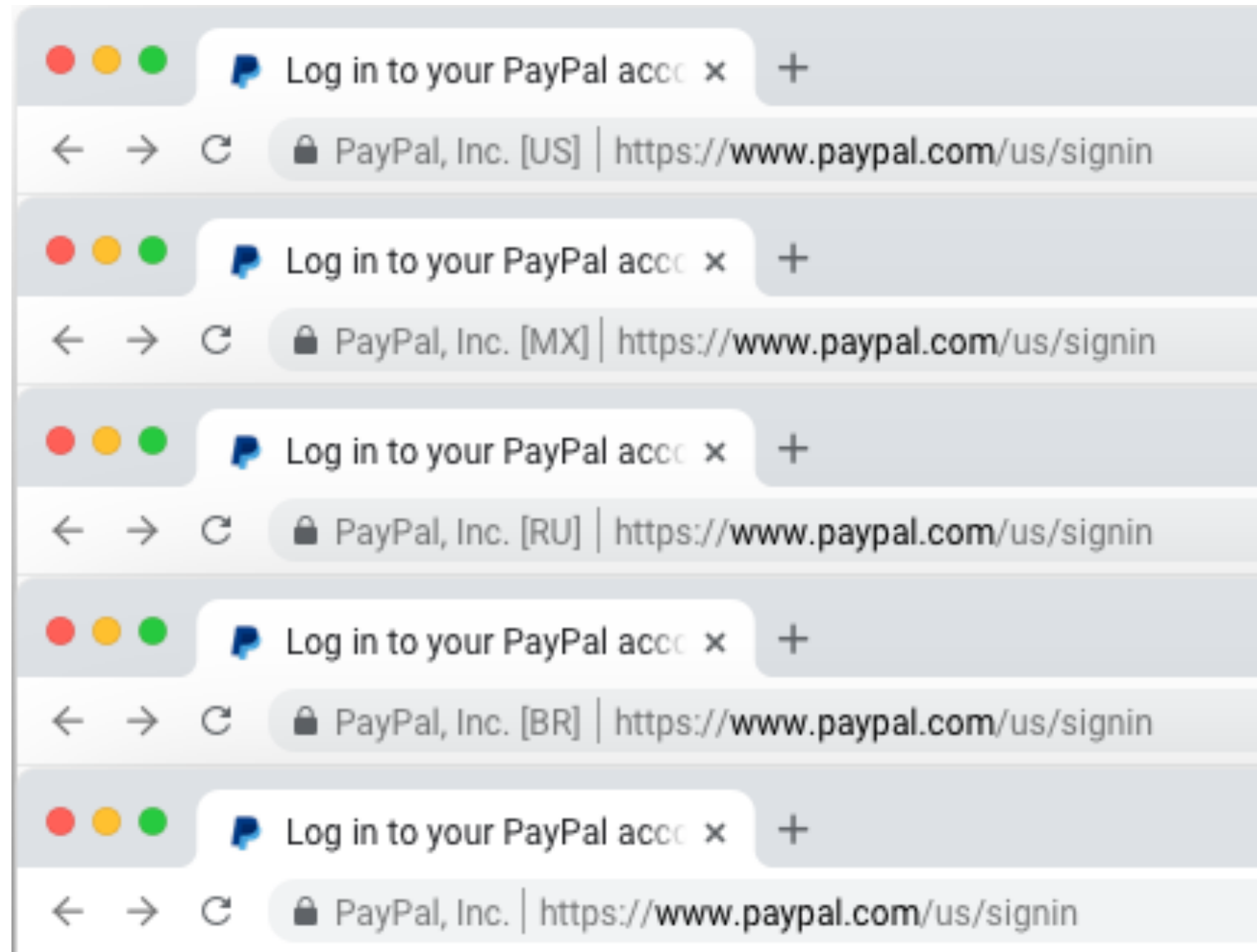
Evaluating the veracity of emails is challenging

- Non-spoofed header?
- Security indicators like DKIM and SPF?
- Personalization, e.g. your name?
- Quality of the text?

Evaluating the veracity of a website is challenging

- Realistic domain name?
- SSL/TLS lock icon?
- “Professional” layout and images?
- Quality and quantity of links?

# Country code



4: Five conditions shown to U.S. participants, manipulating only country code.



# Country code

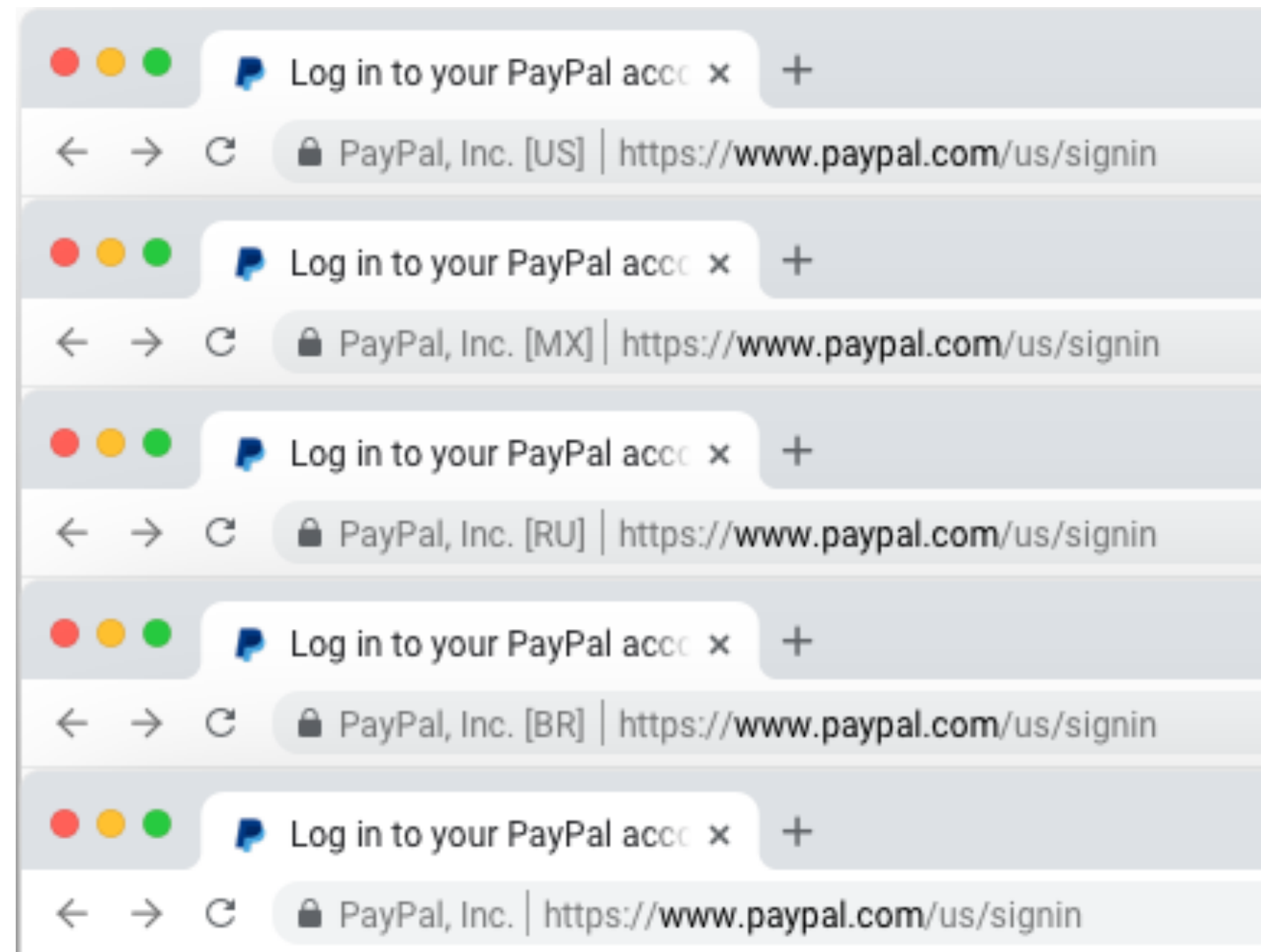


Figure 4: Five conditions shown to U.S. participants, manipulating only country code.

	Cnd 1	Cnd 2	Cnd 3	Cnd 4	Cnd 5
<i>U.S.</i>					
Very comfortable	63%	63%	61%	56%	68%
Somewhat comfortable	30%	24%	25%	28%	21%
Neither comfortable nor uncomfortable	2%	4%	5%	3%	3%
Somewhat uncomfortable	3%	7%	6%	6%	7%
Very uncomfortable	2%	3%	3%	8%	2%
<i>n</i>	121	120	115	117	119
<i>U.K.</i>					
Very comfortable	48%	56%	46%	44%	56%
Somewhat comfortable	31%	33%	36%	39%	35%
Neither comfortable nor uncomfortable	10%	5%	3%	8%	5%
Somewhat uncomfortable	6%	4%	12%	7%	3%
Very uncomfortable	5%	2%	3%	3%	2%
<i>n</i>	125	132	128	132	133

Table 4: Users' comfort levels logging into a webpage with different EV country codes. Cnd 1 is the topmost variation shown in Figure 4 and Cnd 5 is the bottommost.

# Incorrect sign-in page

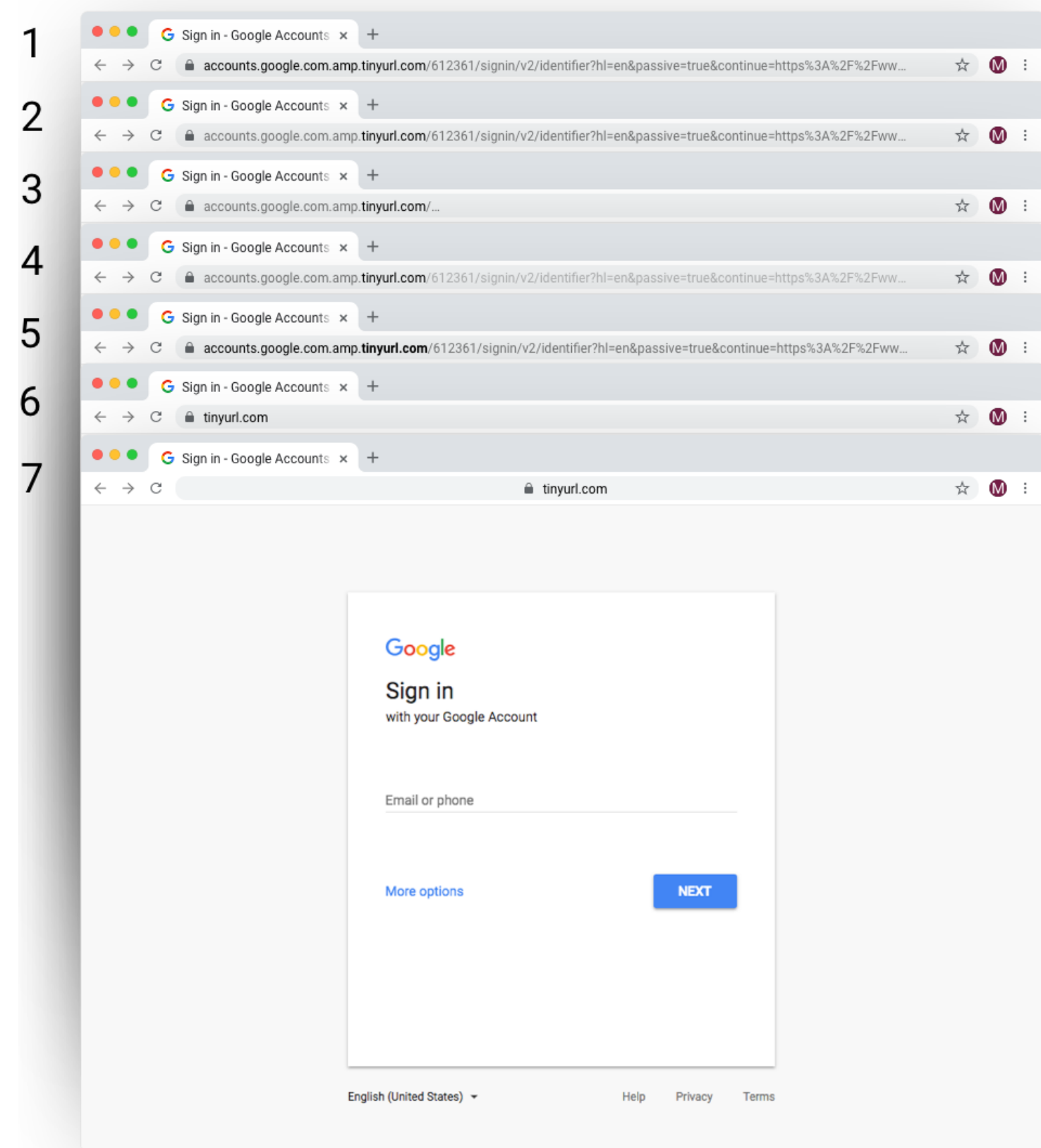


Figure 8: Conditions shown to U.S. participants, manipulating the URL display to emphasize the registrable domain.



# Incorrect sign-in page

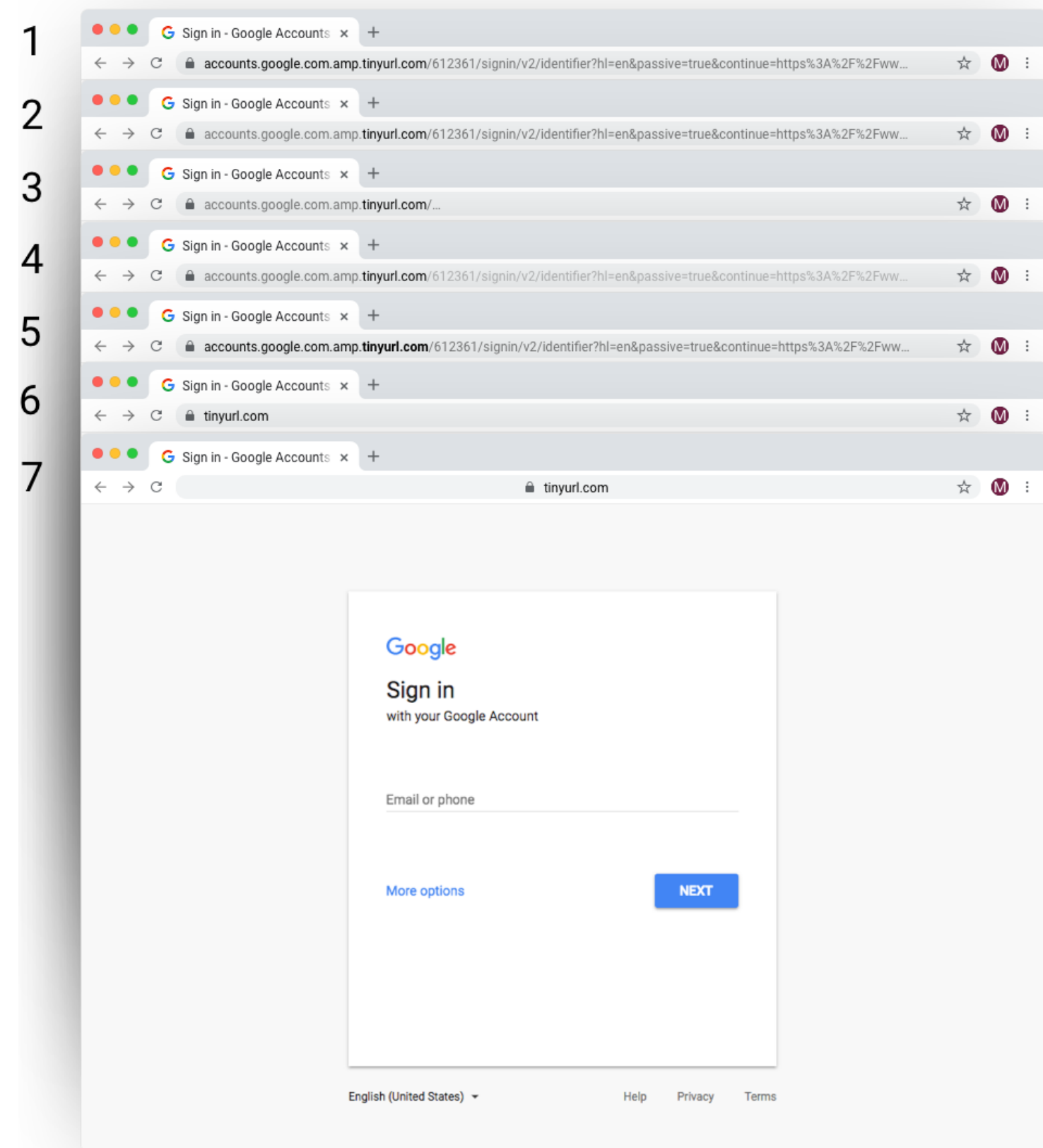


Figure 8: Conditions shown to U.S. participants, manipulating the URL display to emphasize the registrable domain.

	Cnd 1	Cnd 2	Cnd 3	Cnd 4	Cnd 5	Cnd 6	Cnd 7
<i>n</i>	132	127	130	124	128	132	137
<i>Comfortable reasons</i>							
Looks familiar	36%	33%	35%	35%	38%	23%	32%
I trust Google	20%	17%	12%	15%	16%	16%	15%
Page looks simple / easy to use	8%	3%	8%	4%	5%	4%	4%
Site is secured or safe	5%	6%	6%	5%	6%	5%	4%
Page looks normal (unspecified)	2%	1%	0%	2%	2%	2%	1%
URL looks normal	2%	2%	0%	1%	2%	0%	0%
<i>Uncomfortable reasons</i>							
The URL looks funny	23%	27%	33%	27%	30%	32%	33%
I'm not sure the site is safe (unspecified)	2%	7%	2%	7%	2%	13%	4%
I'm unsure where I came from / where I am	3%	3%	2%	0%	2%	3%	1%
Unclear or other	3%	6%	3%	6%	2%	5%	9%

85% of all participants said the website was Google, when in fact, the address said tinyurl.com. 13% of participants correctly identified the website by its URL. 1% described both Google and TinyURL, and 1% provided a different response.

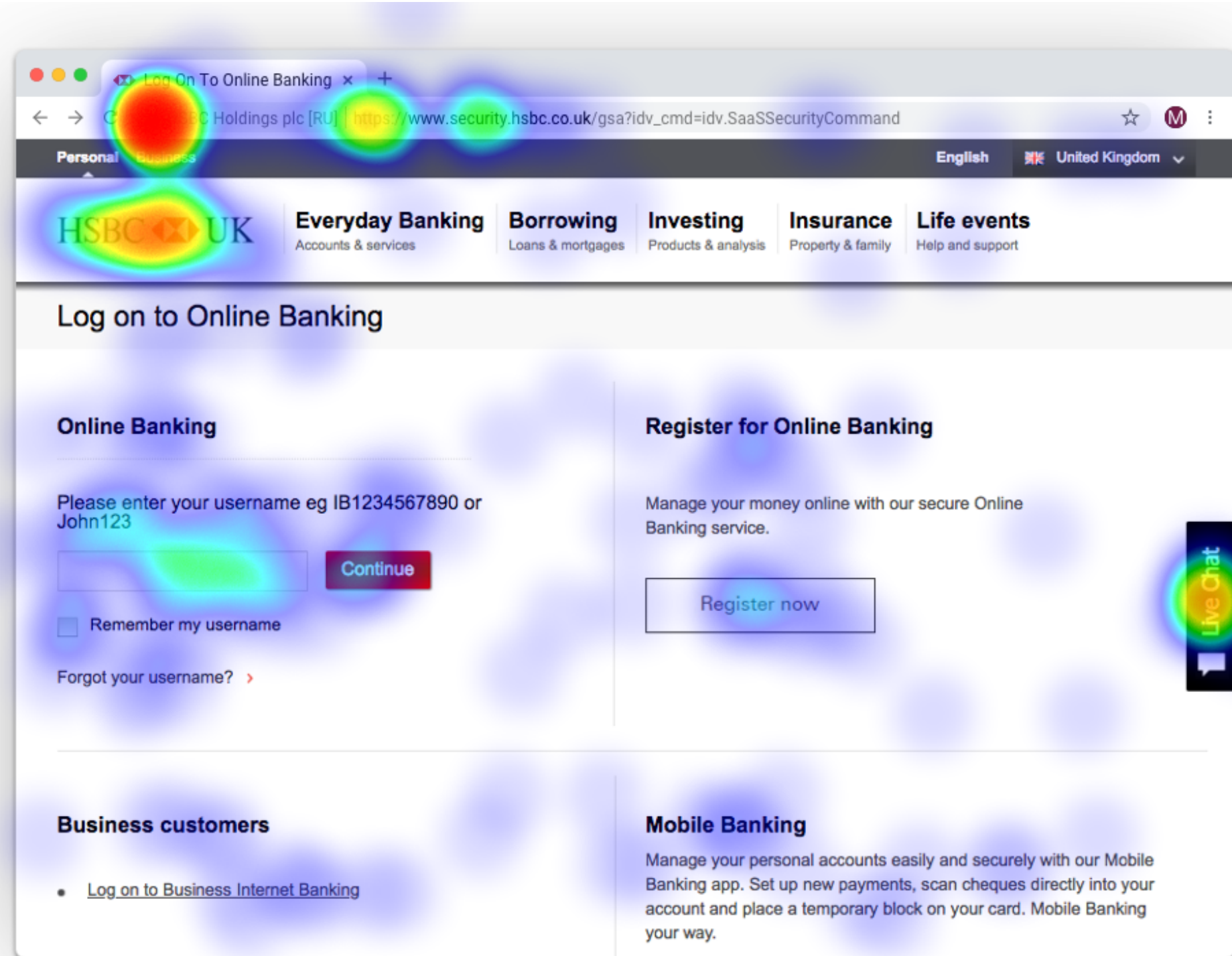


Figure 6: Example click heatmap, displaying what U.K. participants say made them feel comfortable or uncomfortable on a webpage with an RU country code in the EV indicator.

	U.S.					U.K.				
	Cnd 1	Cnd 2	Cnd 3	Cnd 4	Cnd 5	Cnd 1	Cnd 2	Cnd 3	Cnd 4	Cnd 5
<i>n</i>	92	120	93	93	115	83	91	81	83	74
<i>Comfortable reasons</i>										
I'm familiar with this website	33%	26%	31%	40%	33%	10%	7%	6%	7%	14%
I see an HTTPS indicator	32%	16%	23%	19%	17%	27%	25%	21%	23%	35%
URL looks normal	8%	8%	15%	9%	10%	1%	4%	2%	4%	4%
Page looks simple / easy to use	9%	7%	9%	10%	7%	18%	16%	9%	16%	15%
Page looks well-designed	2%	2%	0%	3%	0%	4%	8%	14%	12%	3%
I see an EV certificate	1%	1%	2%	1%	1%	1%	0%	1%	1%	1%
<i>Uncomfortable reasons</i>										
Country code looks strange	0%	6%	5%	8%	0%	0%	1%	5%	0%	0%
Page does not look normal	1%	1%	2%	4%	3%	1%	1%	0%	7%	3%
Page looks bland	1%	1%	4%	1%	3%	10%	2%	1%	5%	1%
URL looks odd	0%	1%	0%	1%	1%	1%	2%	2%	2%	3%
Page looks poorly-designed	0%	0%	0%	0%	0%	6%	7%	9%	7%	4%

Table 5: Sample results of the open-ended question “Can you tell us why you feel that way?” when participants were asked how comfortable they were logging in to a site. Cdn 1 is the topmost condition shown in Figure 4 and Cdn 5 is the bottommost. Full results are shown in the Appendix.



# Training?



MONEY &  
CREDIT

HOMES &  
MORTGAGES

HEALTH &  
FITNESS

JOBS &  
MAKING MONEY

PRIVACY, IDENTITY &  
ONLINE SECURITY

SCAMS

▶ BLOG  
▶ VIDEO & MEDIA

## Four Steps to Protect Yourself From Phishing

**1. Protect your computer by using security software.** Set the [software to update automatically](#) so it can deal with any new security threats.

**2. Protect your mobile phone by setting software to update automatically.** These updates could give you critical protection against security threats.

**3. Protect your accounts by using multi-factor authentication.** Some accounts offer extra security by requiring two or more credentials to log in to your account. This is called [multi-factor authentication](#). The additional credentials you need to log in to your account fall into two categories:

- Something you have — like a passcode you get via text message or an authentication app.
- Something you are — like a scan of your fingerprint, your retina, or your face.

Multi-factor authentication makes it harder for scammers to log in to your accounts if they do get your username and password.

**4. Protect your data by backing it up.** [Back up your data](#) and make sure those backups aren't connected to your home network. You can copy your computer files to an external hard drive or cloud storage. Back up the data on your phone, too.











# Methodology

Participants were asked to role play as another person

- Given this fake person's wallet, containing ID, a credit card, a social security card, and a note containing login credentials for Amazon and Paypal
- Told to read this person's mail and respond to them normally

Inbox contents: Eight total messages

- Three phishing
  - Urgent request from "Citibank", link [www.citicard.com](http://www.citicard.com), actual URL [www.citibank-accountonline.com](http://www.citibank-accountonline.com)
  - Reset password from "Paypal", link "Click here to activate", actual URL [www.payaccount.me.uk](http://www.payaccount.me.uk)
- One 419 scam



# Participants

20 total

- 15 females
- Age 18 – 65 (mean 27)
- 50% white, 25% African American, 15% Asian
- 95% used e-commerce sites
- 70% used online banking
- 25% reported being victims of fraud in the past

# Email Decision Strategies

Email	Legit?	% Suspicious
Meeting	Real	0%
“Cool Pic”	Real	15%
Amazon	Real	25%
Citibank	Phishing	74%
“Great Article”	Malware	85%
Paypal	Phishing	70%
Amazon	Phishing	47%
“Katrina”	419 Scam	95%



# Email Decision Strategies

Email	Legit?	% Suspicious
Meeting	Real	0%
"Cool Pic"	Real	15%
Amazon	Real	25%
Citibank	Phishing	74%
"Great Article"	Malware	85%
Paypal	Phishing	70%
Amazon	Phishing	47%
"Katrina"	419 Scam	95%

## Three identified strategies

1. Is the email personalized and grammatically correct?
  - Somewhat good at identifying malicious email

# Email Decision Strategies

Email	Legit?	% Suspicious
Meeting	Real	0%
“Cool Pic”	Real	15%
Amazon	Real	25%
Citibank	Phishing	74%
“Great Article”	Malware	85%
Paypal	Phishing	70%
Amazon	Phishing	47%
“Katrina”	419 Scam	95%

## Three identified strategies

1. Is the email personalized and grammatically correct?
  - Somewhat good at identifying malicious email
2. Do I have an account with this business?
  - Not a good strategy



# Email Decision Strategies

Email	Legit?	% Suspicious
Meeting	Real	0%
“Cool Pic”	Real	15%
Amazon	Real	25%
Citibank	Phishing	74%
“Great Article”	Malware	85%
Paypal	Phishing	70%
Amazon	Phishing	47%
“Katrina”	419 Scam	95%

## Three identified strategies

1. Is the email personalized and grammatically correct?
  - Somewhat good at identifying malicious email
2. Do I have an account with this business?
  - Not a good strategy
3. Companies send email
  - Extremely naïve, terrible strategy

# Sensitivity to Phishing Cues

Cue

Spoofed “from” address

Broken image links on the website

Strange URL



# Interpretation of Security Warnings

Message	Seen?	Proceed	Stop	Depends
Leaving secure site	71%	58%	0%	42%
Insecure form submission	65%	45%	35%	20%
Self-signed certificate	42%	32%	26%	42%
Entering secure site	38%	82%	0%	18%

Overall, people tend to ignore warnings

Participants were often inured

- “I get these warnings on my school website, so I just ignore them”

“Entering secure site” sometimes made people more suspicious!

- The paradox of security

# “Why Phishing Works”

- Rachna Dhamija, J. D. Tygar, Marti Hearst
- 2006
- Similar study: showed 20 websites to 22 participants, asked them to identify phishing sites and explain why they thought so



# Methodology

- 20 websites, first 19 in random order
  - 7 legit
  - 9 representative, real phishing sites
  - 3 phishing sites crafted by the researchers
  - Final site: self-signed SSL certificate
- All websites were fully functional

# Participants and Overall Results

- 22 participants
  - 45.5% female
  - Age 18—56 (mean 30)
  - 73% had a bachelors degree
  - 50% used Internet Explorer (remember, its 2006)
- Results: correct identifications ranged from 6—18 (out of 19)
  - No correlation with sex, age, education level, hours of computer experience, or browser choice



# Identification Strategies

Strategy	# of Participants	Correct Judgements
Website content only	5	6—9
+ Domain name	8	10—13
+ HTTPS	2	8—16
+ Padlock icon	5	12—17
+ Checked the certificate	2	10—18

# “Who Falls for Phish? A Demographic Analysis of Phishing Susceptibility and Effectiveness of Interventions”

- Steve Sheng, Mandy Holbrook, Ponnurangam Kumaraguru, Lorrie Cranor, Julie Downs
- 2010
- Recruited 1000 people to role play as another person
  1. Look through an inbox and deal with the mail
  2. Possibly receive an educational intervention
  3. Look through a second inbox and deal with it

# Results

Condition	Falling for phishing attacks		Clicking on legit websites	
	1 <sup>st</sup> role play	2 <sup>nd</sup> role play	1 <sup>st</sup> role play	2 <sup>nd</sup> role play
No training	50%	47%	70%	74%
Popular training	46%	26%	67%	61%
Anti-Phishing Phil	46%	29%	73%	73%
PhishGuru Cartoon	47%	31%	70%	64%
Phil+PhishGuru	47%	26%	68%	59%

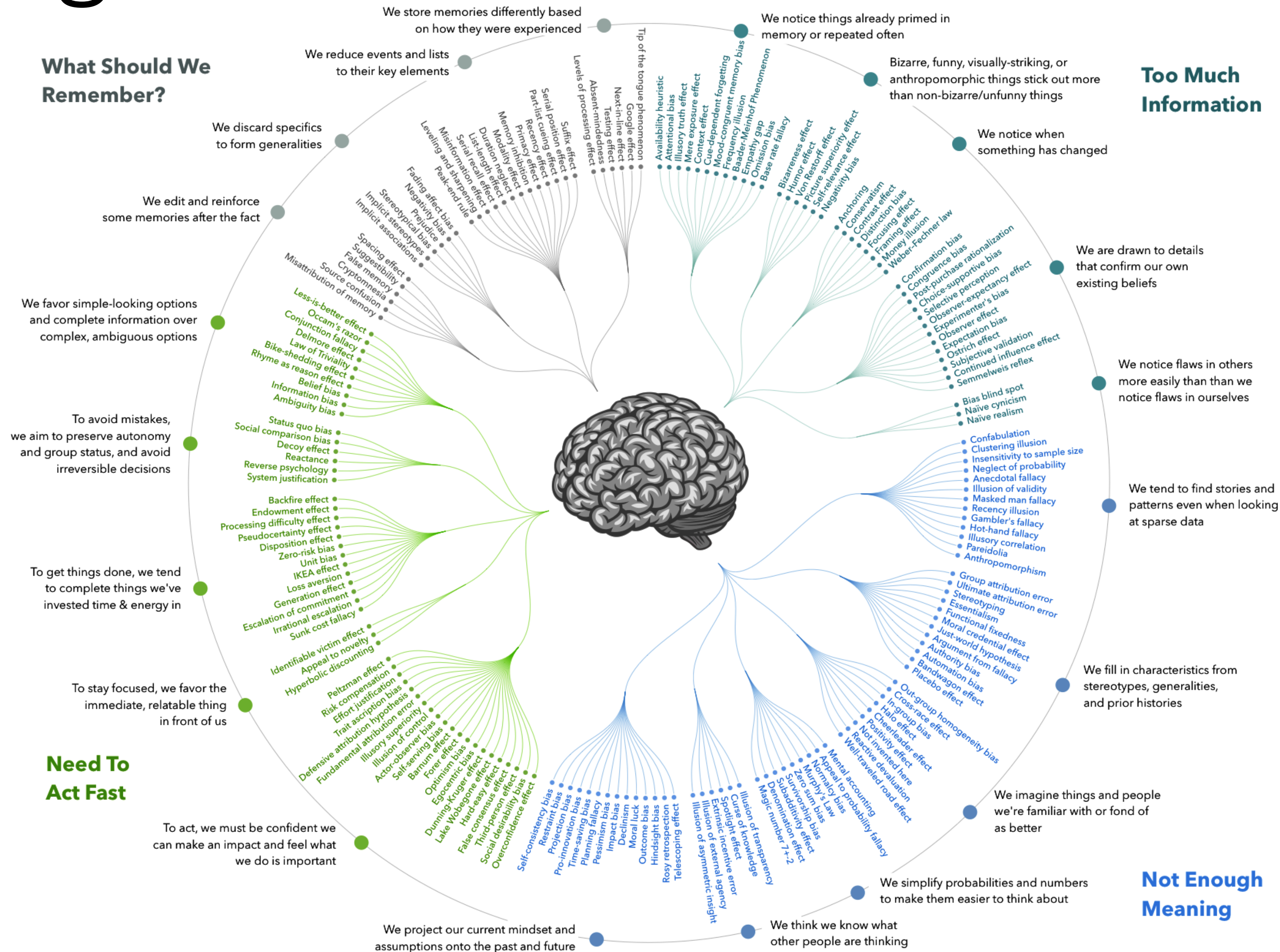


# Results

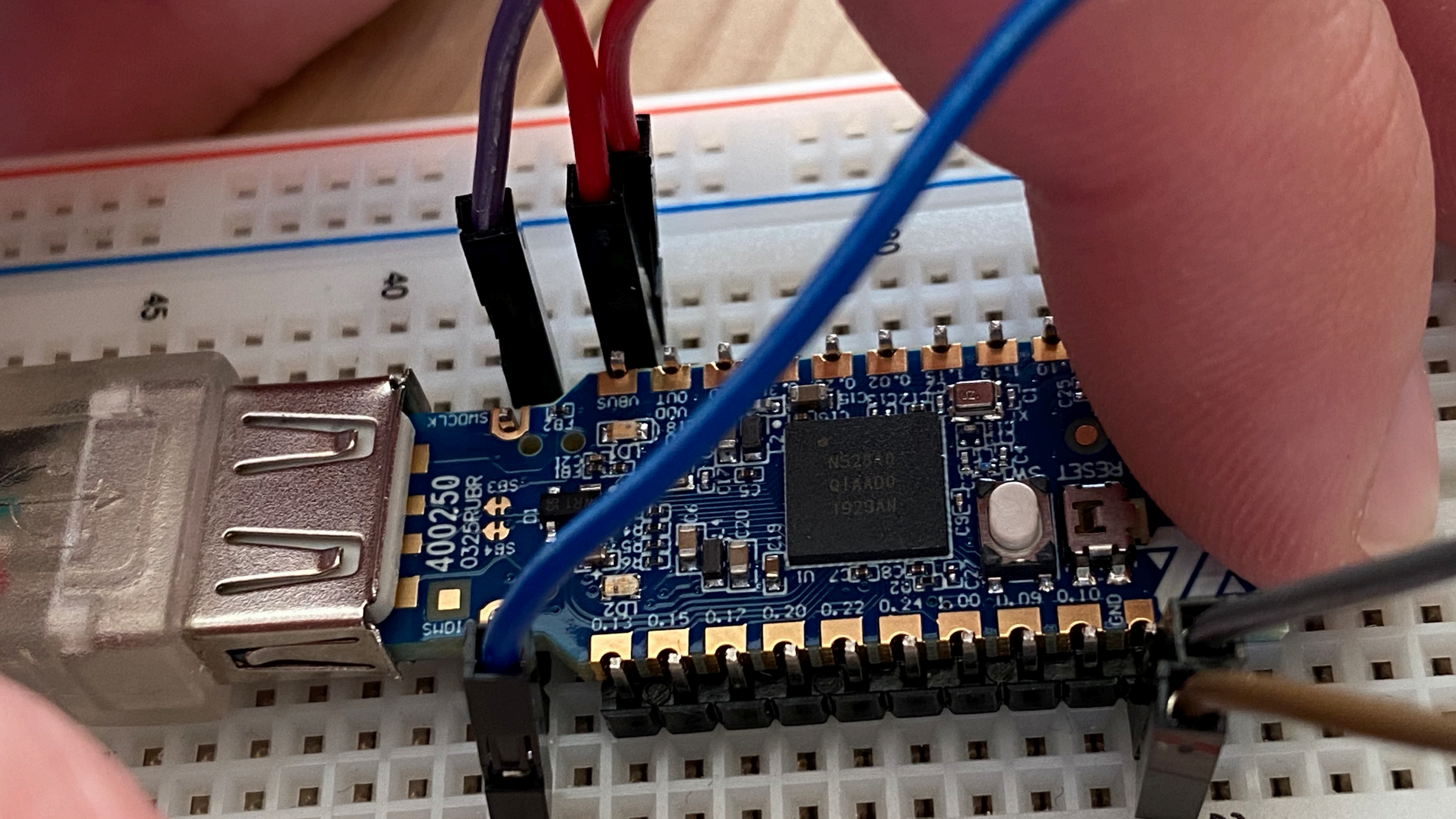
Condition	Falling for phishing attacks		Clicking on legit websites	
	1 <sup>st</sup> role play	2 <sup>nd</sup> role play	1 <sup>st</sup> role play	2 <sup>nd</sup> role play
No training	50%	47%	70%	74%
Popular training	46%	26%	67%	61%
Anti-Phishing Phil	46%	29%	73%	73%
PhishGuru Cartoon	47%	31%	70%	64%
Phil+PhishGuru	47%	26%	68%	59%

- Before training: 47% of attacks were successful, on average
- After training: only 28% were successful on average (40% improvement)
- But, willingness to click on real links also dropped slightly

# Heuristics → Cognitive Bias







400250  
0325RUBR

N52840  
01A00  
1929AM

45

40

10MS

RESET

GND

01.0 50.0 00.0 0.24 0.22 0.20 0.17 0.15 0.13 0.11 0.09 0.07 0.05 0.03 0.02 0.01

0.02 0.22 0.24 0.22 0.20 0.17 0.15 0.13 0.11 0.09 0.07 0.05 0.03 0.02 0.01

0.02 0.22 0.24 0.22 0.20 0.17 0.15 0.13 0.11 0.09 0.07 0.05 0.03 0.02 0.01

0.02 0.22 0.24 0.22 0.20 0.17 0.15 0.13 0.11 0.09 0.07 0.05 0.03 0.02 0.01

0.02 0.22 0.24 0.22 0.20 0.17 0.15 0.13 0.11 0.09 0.07 0.05 0.03 0.02 0.01

0.02 0.22 0.24 0.22 0.20 0.17 0.15 0.13 0.11 0.09 0.07 0.05 0.03 0.02 0.01

0.02 0.22 0.24 0.22 0.20 0.17 0.15 0.13 0.11 0.09 0.07 0.05 0.03 0.02 0.01

0.02 0.22 0.24 0.22 0.20 0.17 0.15 0.13 0.11 0.09 0.07 0.05 0.03 0.02 0.01

0.02 0.22 0.24 0.22 0.20 0.17 0.15 0.13 0.11 0.09 0.07 0.05 0.03 0.02 0.01

0.02 0.22 0.24 0.22 0.20 0.17 0.15 0.13 0.11 0.09 0.07 0.05 0.03 0.02 0.01



# Cognitive Biases

## Behavioral Biases

### Belief bias

- Evaluation of an argument is based on the believability of the conclusion

### Confirmation bias

- search out information that confirms existing preconceptions

### Courtesy bias

- Urge to avoid offending people

### Framing effect

- Drawing different conclusions from the same info, based on how it was presented

### Stereotyping

## Social Biases

### Authority bias

- Tendency to believe and be influenced by authority figures, regardless of content

### Halo effect

- Tendency for positive personality traits from one area to “spill” into another

### Ingroup bias

- Tendency to give preferential treatment to others from your own group

## Memory Biases

### Context effect

- Cognition and memory are dependent on context

### Suggestibility

- Misattributing ideas from the questioner as one's own



# New attacks from the same problem:

1

**LOTTERY WINNER ARRESTED FOR DUMPING \$200,000 OF MANURE ON EX-BOSS' LAWN**



**2,383,021**

**Lottery winner arrested for dumping \$200,000 of manure on ex-boss' lawn**

2

**Barbara Bush, Republican matriarch and former first lady, dies at 92**



**2,290,000**

**Former first lady Barbara Bush dies at 92**

3

**WOMAN SUES SAMSUNG FOR \$1.8M AFTER CELL PHONE GETS STUCK INSIDE HER VAGINA**



**1,304,430**

**Woman sues Samsung for \$1.8M after cell phone gets stuck inside her vagina**

4

**BREAKING: Michael Jordan Resigns From The Board At Nike- Takes 'Air Jordans' With Him**



**911,336**

**BREAKING: Michael Jordan Resigns From The Board At Nike-Takes 'Air Jordans' With Him**

5

**Donald Trump Ends School Shootings By Banning Schools**



**830,116**

**Donald Trump Ends School Shootings By Banning Schools**

6

**Florida Man Arrested For Tranquilizing And Raping Alligators In Everglades**



**824,137**

**Florida Man Arrested For Tranquilizing And Raping Alligators In Everglades**

7



**Two altar boys were arrested for putting weed in the censer-burner**

**797,628**

**Two altar boys were arrested for putting weed in the censer-burner**

8

**North Korea Agrees To Open Its Doors To Christianity**



**760,314**

**North Korea Agrees To Open Its Doors To Christianity**

9

**Man Eats Girlfriend For The First Time Dies From**



**633,000**

**Man Eats Girlfriend For The First Time Dies From**

10



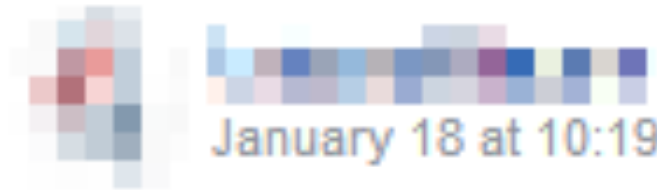
**Muslim Figure: "We Must Have Pork-Free Menus Or We Will Leave U.S." How Would You Respond This?**

**631,589**

**Muslim Figure: "We Must Have Pork-Free Menus Or We Will Leave U.S." How Would You Respond This?**



# Which biases?



January 18 at 10:19am · 🌐



<http://www.usaprides.com/.../denzel-washington-criminal-in-c.../>



## Denzel Washington: 'Criminal-In-Chief' Obama 'Tore Heart Out Of America'

Former president Barack Obama ran the United States "like a banana republic" as "criminal-in-chief" and enriched himself and his cronies at the expense of the rest...

USAPRIDES.COM



👍❤️😱 227

Chronological ▾



# Which biases?

January 18 at 10:19am · 🌐

<http://www.usaprides.com/.../denzel-washington-criminal-in-c.../>



**Denzel Washington: 'Criminal-In-Chief' Obama 'Tore Heart Out Of America'**

Former president Barack Obama ran the United States "like a banana republic" as "criminal-in-chief" and enriched himself and his cronies at the expense of the rest...

USAPRIDES.COM

👍 Like

💬 Comment

➦ Share


👍❤️😱 227

Chronological ▾

... Add featured photos

+ Add Instagram, Websites, Other Links

📷 Photos



👤 Friends

📁 Featured albums

English (UK) · English (US) · Polski · Español · Português (Brasil) +

Privacy · Terms · Advertising · AdChoices · Cookies · More ▾

Leo Porter  
1 June · 🌐 · 👤 ▾

<https://www.ncscooper.com/trumps-health-deteriorates-as-wh.../>



**Trump's Health Deteriorates as White House Pressures Mount**

Health experts are counseling the President to take it easy.

NCSCOOPER.COM | BY RANDALL FINKELSTEIN

👍 Like   💬 Comment   ➦ Share



Table 1: Top fake news domains: Comparing fall 2016 to fall 2018

All (2016)		Democrats (2016)		Republicans (2016)		
Domain	Total visits	Domain	Total visits	Domain	Total visits	
1	ijr.com	4361	bipartisanreport.com	1896	ijr.com	3130
2	bipartisanreport.com	2131	ijr.com	201	angrypatriotmovement.com	1202
3	angrypatriotmovement.com	1480	endingthefed.com	162	redstatewatcher.com	992
4	redstatewatcher.com	1135	greenvillegazette.com	76	endingthefed.com	792
5	endingthefed.com	1109	redstatewatcher.com	50	usherald.com	538
6	conservativedailypost.com	597	embols.com	39	conservativedailypost.com	529
7	usherald.com	573	truthfeed.com	38	chicksontheright.com	428
8	chicksontheright.com	542	dailywire.com	37	tmn.today	323
9	dailywire.com	475	worldpoliticus.com	36	libertywritersnews.com	309
10	truthfeed.com	430	usanewsflash.com	21	dailywire.com	307

All (2018)		Democrats (2018)		Republicans (2018)		
Domain	Total visits	Domain	Total visits	Domain	Total visits	
1	dailywire.com	1322	dailywire.com	67	dailywire.com	1111
2	ilovemyfreedom.org	179	bipartisanreport.com	28	ilovemyfreedom.org	171
3	conservativedailypost.com	165	dailyoccupation.com	4	conservativedailypost.com	126
4	tmn.today	42	tmn.today	2	tmn.today	39
5	bipartisanreport.com	33	awarenessact.com	1	ijr.com	19
6	ijr.com	20	ilovemyfreedom.org	1	ipatriot.com	10
7	ipatriot.com	10			truthfeed.com	4
8	awarenessact.com	5			conservativefiringline.com	2
9	conservativefiringline.com	4			awarenessact.com	1
10	dailyoccupation.com	4			bipartisanreport.com	1

Online traffic statistics among YouGov Pulse panel members. Fake news consumption is measured as visiting domains that were coded as pro-Trump or pro-Clinton from among those identified by Allcott and Gentzkow 2017 (2016 definition).