2550 Intro to cybersecurity

L14: Cognitive bias

Ran Cohen/abhi shelat

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

Google Federal Bureau of Investigation lowell

Sign in

All News Maps Images Videos More Settings Tools

About 205,000 results (0.62 seconds)

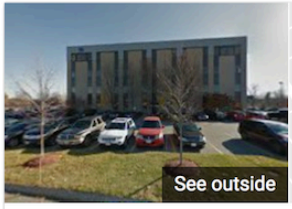
Federal Bureau of Investigation in Lowell, MA - (978) 454-6972 - Buzzfile
www.buzzfile.com/business/FBI-978-454-6972
Federal Bureau of Investigation, which also operates under the name **FBI**, is located in **Lowell**, Massachusetts. This organization primarily operates in the ...

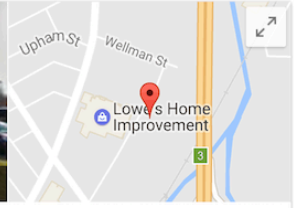
Federal Bureau of Investigation in Lowell, MA - (978) 454-6972 - Buzzfile
www.buzzfile.com/business/Federal-Bureau-of-Investigation-978-454-6972
Federal Bureau of Investigation is located in **Lowell**, Massachusetts. This organization primarily operates in the General Government Administration business ...

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. ... History of the **FBI's** Boston, Massachusetts Field Office. More ... **Lowell**, MA. Counties ...

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

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

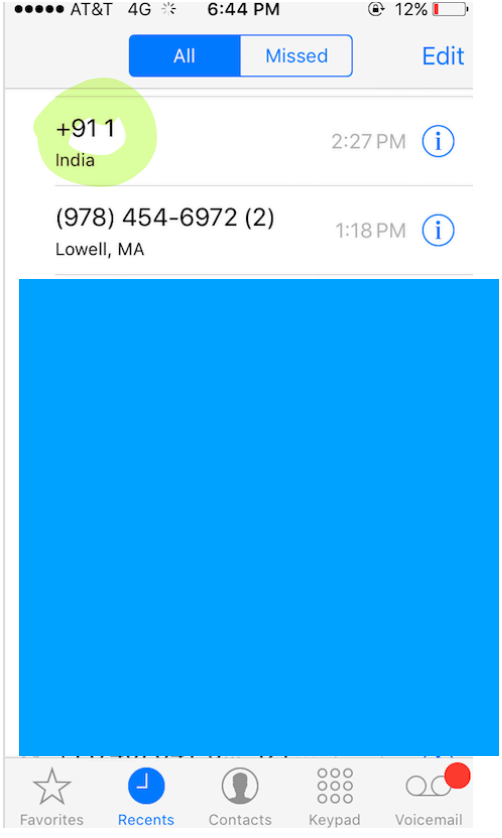
Reviews

Write a review Add a photo

Be the first to review

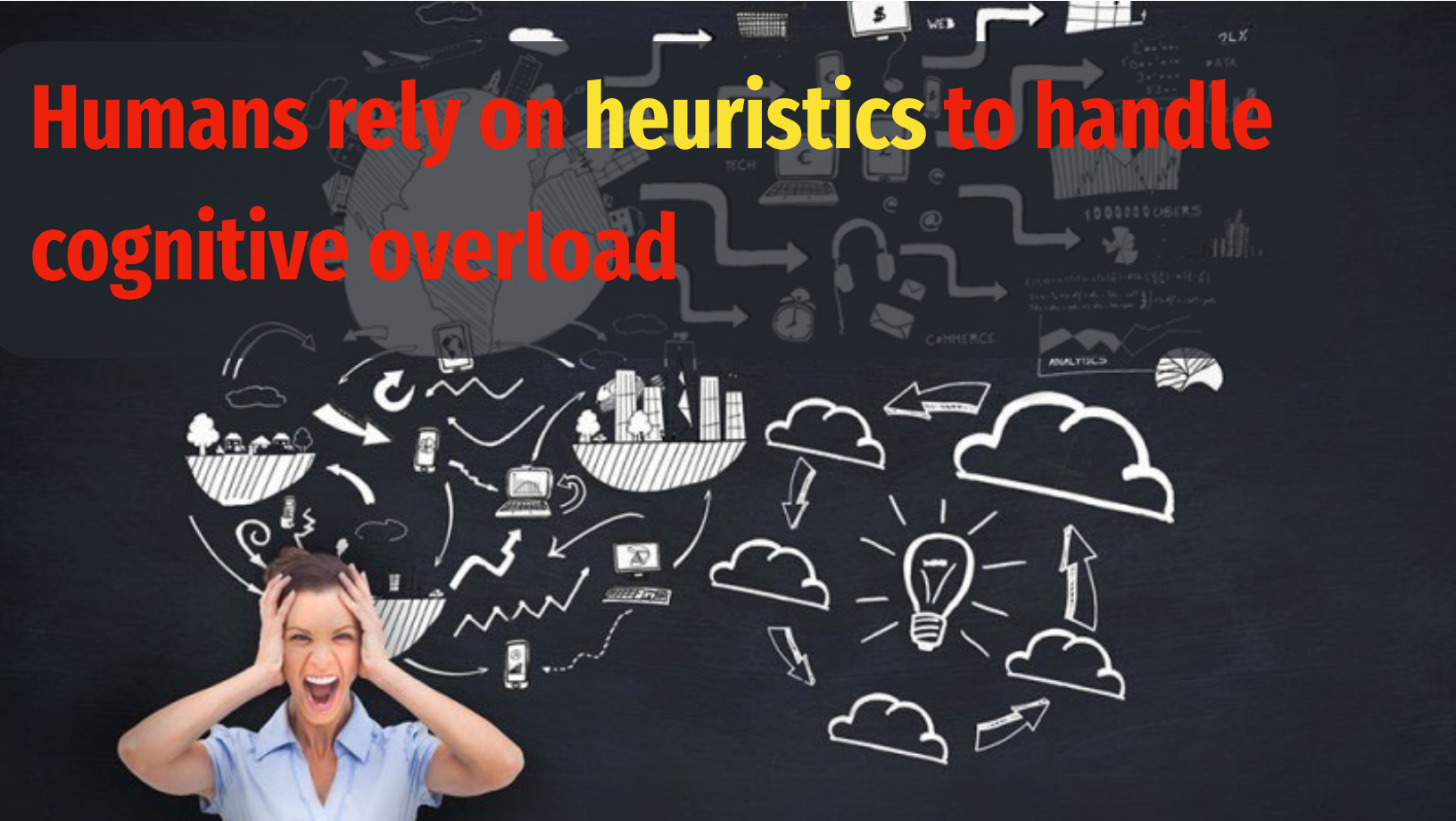
Feedback

the similarity of two search result lists 158, 391

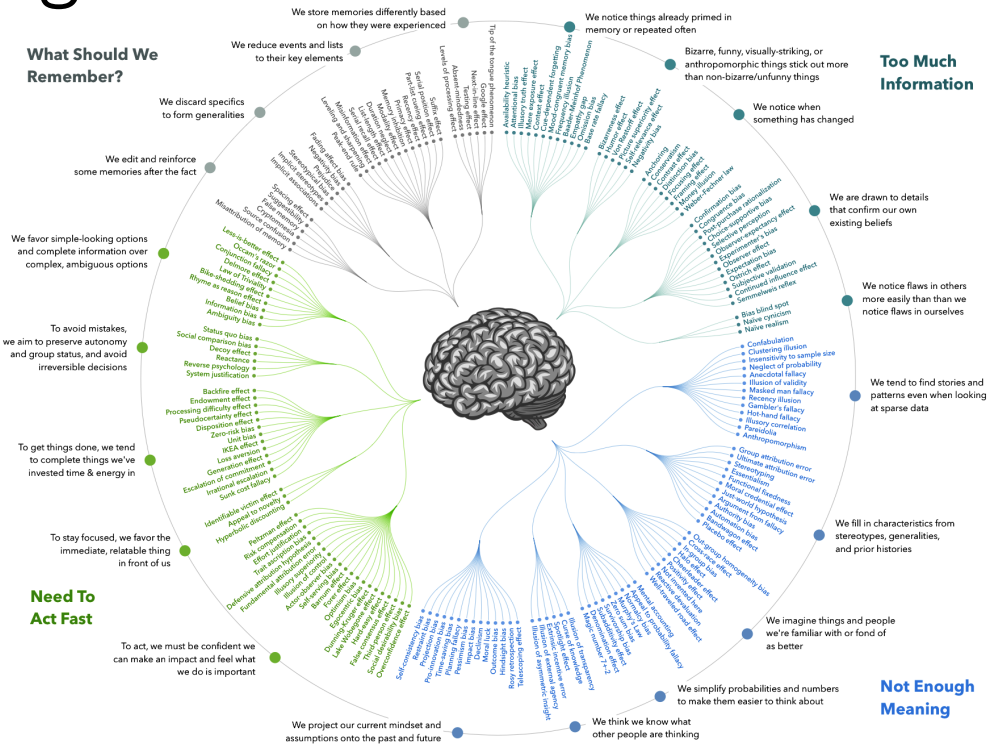

AT&T 4G 6:44 PM 12%
All
Missed
Edit
+91 1
India
2:27 PM
(978) 454-6972 (2)
Lowell, MA
1:18 PM
Favorites
Recents
Contacts
Keypad
Voicemail

Why so effective?

Humans rely on heuristics to handle cognitive overload



Heuristics —> Cognitive Bias



DESIGNHACKS.CO · CATEGORIZATION BY BUSTER BENSON · ALGORITHMIC DESIGN BY JOHN MANOOGIAN III (JM3) · DATA BY WIKIPEDIA

Cognitive Biases

Behavioral Biases

Belief bias:
Evaluation of an argument is tied to the believability of the conclusion.

Confirmation bias
- people search for information that confirms their beliefs.

Courtesy bias
- urge to be polite

Framing effect
- Drawing different conclusions from the same data based on how it is presented.

Anchoring effect
- people establish beliefs, and then are slow to change even after observing contradictory evidence

Social Biases

Authority bias
- give more credibility to authority

Halo effect
- tend to let positive attributes "spillover" to other characteristics.

Ingroup bias

Memory Biases

Context effect

Suggestibility
"Inception"

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

Anchoring effect
- Humans make simple basic probability assessments and are slow to update based on observation

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

Human social perception is a constructive process

versus objective.

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."

Quote from "Ghost in the Wires" by Kevin Mitnick

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."

Courtesy bias

Suggestability

Quote from "Ghost in the Wires" by Kevin Mitnick

Elicitation

SIM HIJACKING

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

Adapted from "Social Engineering: The Art of Human Hacking"

Persuasion

(SALES)

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

Leveraging Cognitive Overload

Crafting a story isn’t just for pretexting

- Useless details obfuscate true intentions
- Increases cognitive load in the victim, increasing susceptibility

Leveraging Cognitive Overload

Crafting a story isn't just for pretexting

- Useless details obfuscate true intentions
- Increases cognitive load in the victim, increasing susceptibility

You are the bus driver. At your first stop, you pick up 29 people. On your second stop, 18 of those 29 people get off, and at the same time 10 new passengers arrive. At your next stop, 3 of those 10 passengers get off, and 13 new passengers come on. On your fourth stop 4 of the remaining 10 passengers get off, 6 of those new 13 passengers get off as well, then 17 new passengers get on.

What is the color of the bus driver's eyes?

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

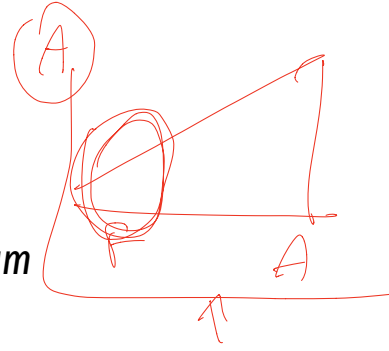
Kevin On Follow-through

“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

In class example

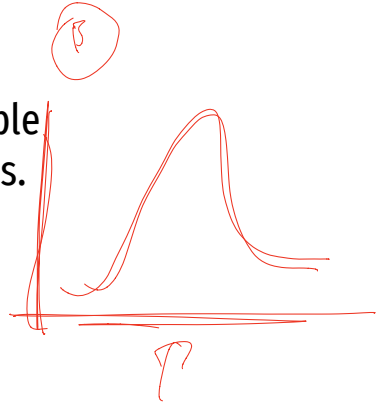
Zero sum bias



"The experiments reported here were designed to test the hypothesis that people are prone to perceive a competition for limited resources (i.e., employ a *zero-sum heuristic*) even when there are unlimited resources available."

...

A plausible explanation for the findings is that a zero-sum heuristic evolved as a cognitive adaptation to enable successful intra-group competition for limited resources. Implications for understanding inter-group interaction are also discussed.



Zero sum bias

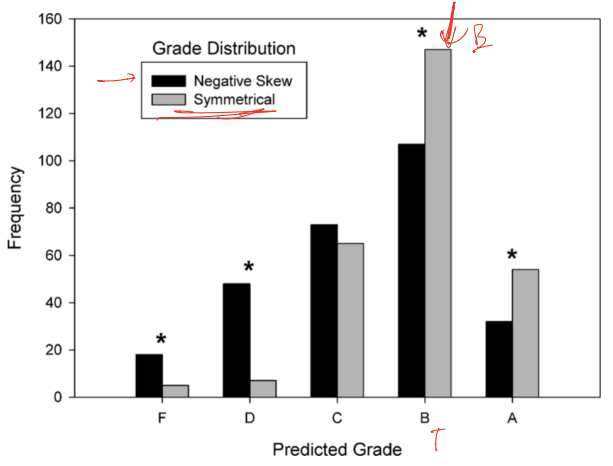


FIGURE 2 | Predicted grade frequency as a function of grade distribution condition in Experiment 1. Distribution condition had a significant influence on grade judgments, particularly at those grade levels marked with an asterisk (indicating $p < 0.05$). Negative skew increased low grade predictions and decreased high grade predictions, suggesting a zero-sum bias.

Zero-sum bias: perceived competition despite unlimited resources

Daniel V. Meegan

Halo effect

3. Thorndike, E.L. (1920). A constant error in psychological ratings. *Journal of Applied Psychology, 4*(1), 25–29. https://doi.org/10.1037/h0071663.

4. Harvey, S. M. (1938). A preliminary investigation of the interview. *British Journal of Psychology. General Section, 28*(3), 263–287. https://doi.org/10.1111/j.2044-8295.1938.tb00874.

Attractiveness

Journal Information
Journal TOC

Search APA PsycNet

APA PsycArticles: Journal Article

Name stereotypes and teachers' expectations.

Harari, H., & McDavid, J. W. (1973). Name stereotypes and teachers' expectations. *Journal of Educational Psychology, 65*(2), 222–225. https://doi.org/10.1037/h0034978

Predicted that teachers' evaluations of children's performance would be systematically associated with stereotyped perceptions of first names. Short essays actually written by 5th-grade students were presented for evaluation to 80 female teachers (age range 20-45) and 80 female undergraduates. Authorship of the essays was randomly linked with boys and girls with common, popular, and attractive names as well as with rare, unpopular, and unattractive names. As expected, the attributed quality of each essay was higher when essays were authored by names associated with positive stereotypes. This stereotype bias was more pronounced for experienced teachers than for inexperienced undergraduates, and the effect was clearer for boys' names than for girls' names. (APA PsycInfo Database Record (c) 2016 APA, all rights reserved)

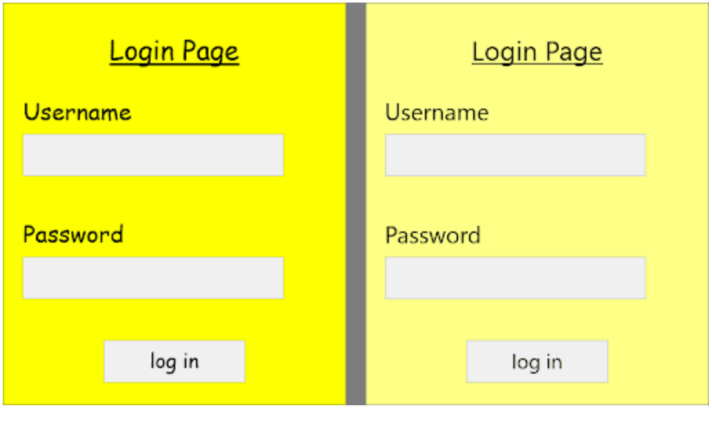
TABLE 1

MEAN NUMERICAL SCORE RATINGS BY TEACHERS

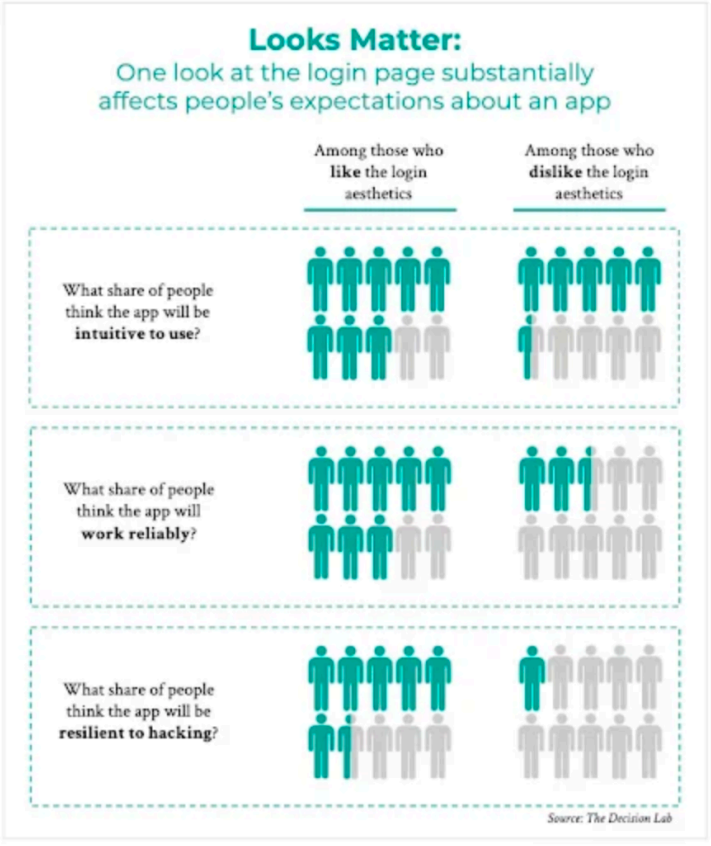
Name	Score	Essay content	Score	Presentation sequence	Score
		Boys			
David	83.55*	The store	81.02	First	79.95
Michael	80.02	Tarzan	79.70	Second	80.47
Elmer	78.17	The anniversary	79.57	Third	81.25
Hubert	77.97	Kites	78.92	Fourth	81.25
		Girls			
Adelle	86.62*	Shopping	85.37*	First	79.55
Lisa	81.95*	Walking the dog	81.90	Second	83.95*
Karen	80.95	Playing dolls	81.32	Third	84.02*
Bertha	78.35	Planting seeds	79.47	Fourth	80.55

* $p < .05$.

Halo effect experiment



The participants in the experiment were then asked to rate several aspects of the app's expected attributes, as well as its aesthetics. The main findings of this test are summarized in the following infographic:



https://thedecisionlab.com/insights/consumer-insights/the-halo-effect-in-consumer-perception-why-small-details-can-make-a-big-difference/

Case Study: Phishing

Evaluating emails

Evaluating websites

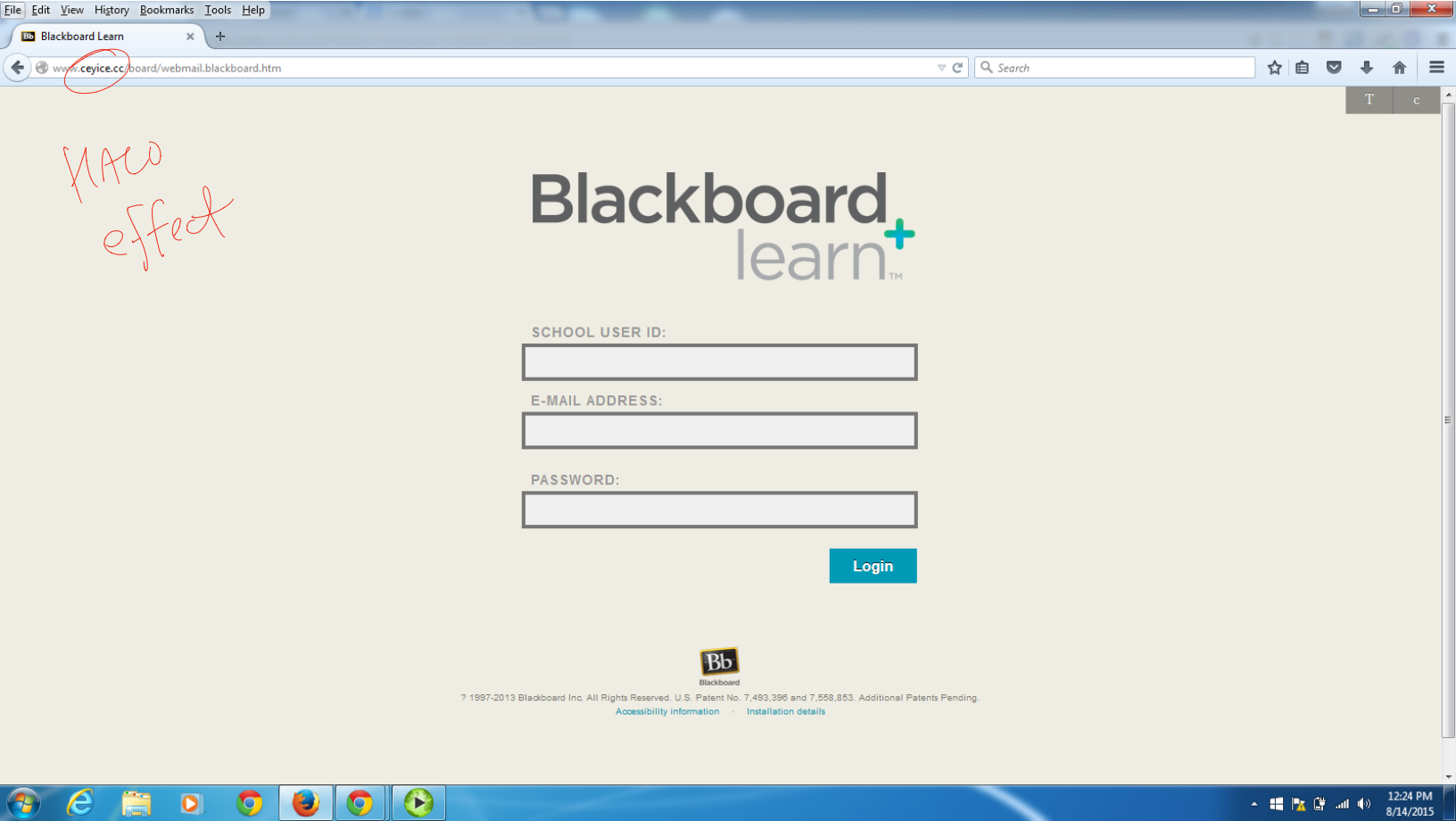
Does training work?

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:* [redacted]ta@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.


File Edit View History Bookmarks Tools Help
Blackboard Learn
www.ceyice.cc/board/webmail.blackboard.htm
Search
T c
HACO effect
Blackboard learn
SCHOOL USER ID:
E-MAIL ADDRESS:
PASSWORD:
Login
Bb
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
12:24 PM
8/14/2015

identify the cognitive biases employed.

-----Original Message-----
From: Peggy Altman [mailto:peggyaltman@usa.com]
Sent: Tuesday, May 16, 2017 6:23 AM
To: You <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

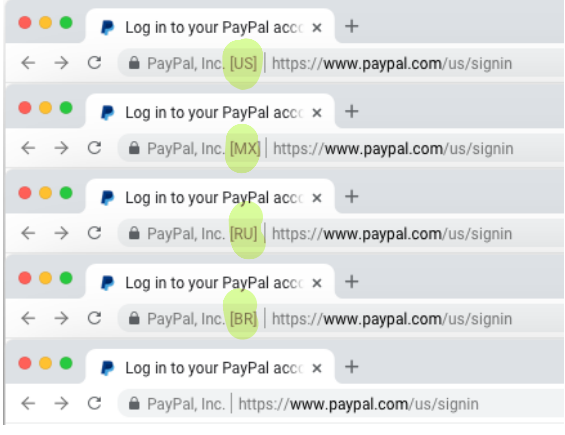
- Non-spoofed header?
- Security indicators like DKIM and SPF?
- Personalization, e.g. your name?
- Quality of the text?

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

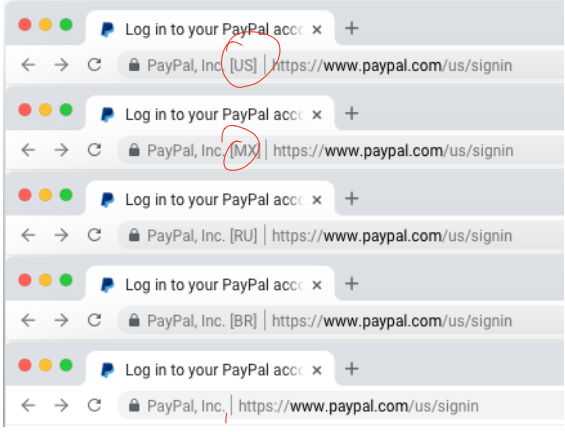
The Web's Identity Crisis:Understanding the Effectiveness of Website Identity Indicators
USENIX 2019, Google



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

Country code

The Web's Identity Crisis:Understanding the Effectiveness of Website Identity Indicators
USENIX 2019, Google



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

	Cnd 1	Cnd 2	Cnd 3	Cnd 4	Cnd 5
U.S.					
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%
n	121	120	115	117	119
U.K.					
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%
n	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.

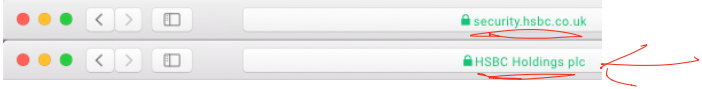


Figure 5: Two conditions shown to U.K. participants, manipulating display of EV to include the site's registrable domain (macOS 10.14) or EV legal entity name (as in macOS 10.13).

Incorrect sign-in page

The Web's Identity Crisis:Understanding the Effectiveness of Website Identity Indicators
USENIX 2019, Google

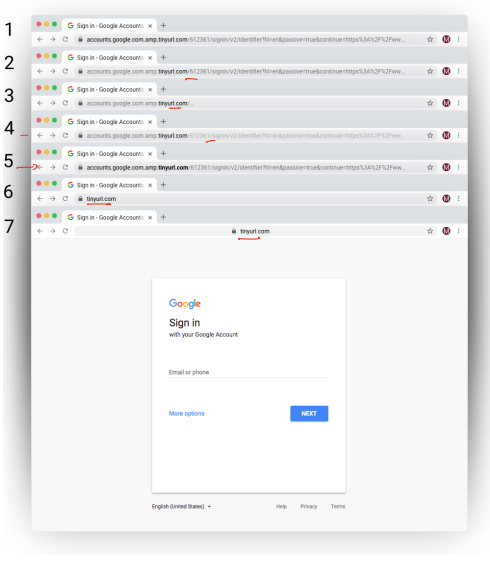


Figure 8: Conditions shown to U.S. participants, manipulating the URL display to emphasize the registrable domain.

Incorrect sign-in page

The Web's Identity Crisis:Understanding the Effectiveness of Website Identity Indicators
USENIX 2019, Google

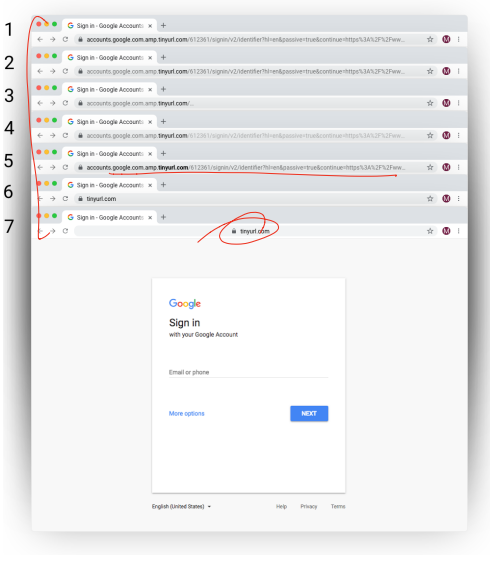


Figure 8: Conditions shown to U.S. participants, manipulating the URL display to emphasize the registrable domain.

	Cnd 1	Cnd 2	Cnd 3	Cnd 4	Cnd 5	Cnd 6	Cnd 7
n	132	127	130	124	128	132	137
Comfortable reasons							
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%
Uncomfortable reasons							
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%

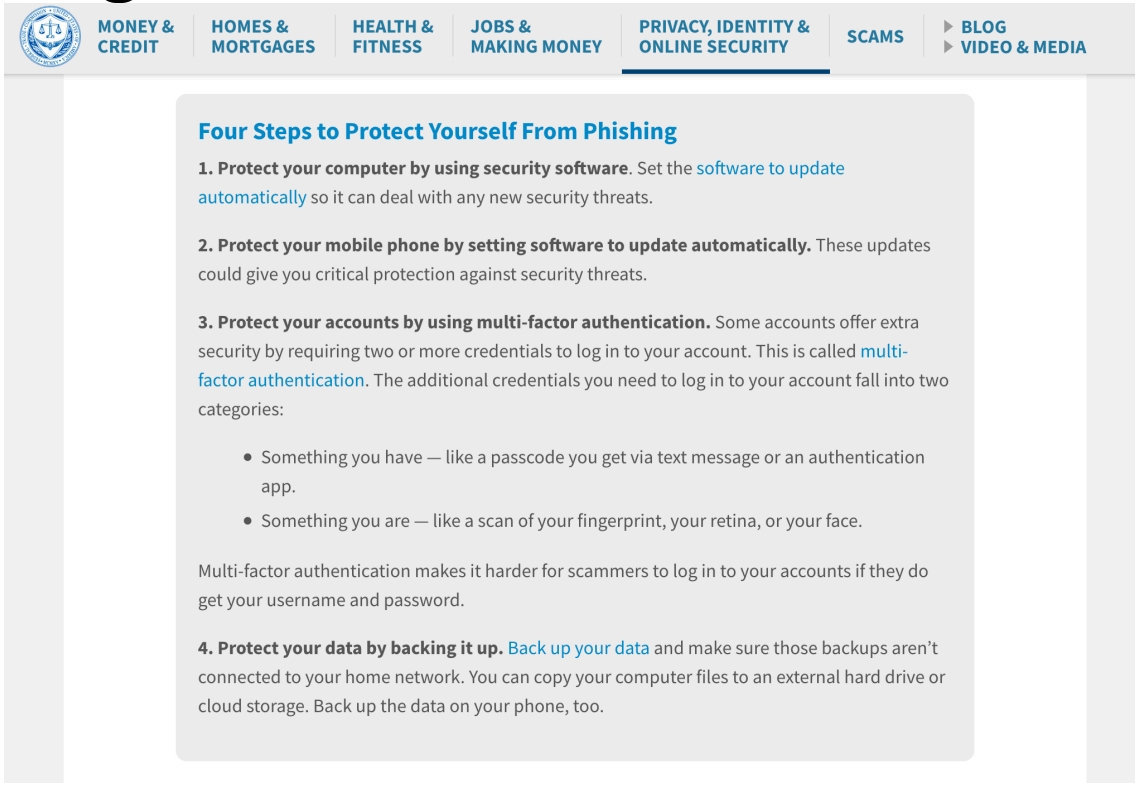
85% of all participants said the website was Google, when in fact, the address said tinyurl.com. 13% of participants correctly identi- fied the website by its URL. 1% described both Google and TinyURL, and 1% provided a different response.

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. Cnd 1	Cnd 2	Cnd 3	Cnd 4	Cnd 5	U.K. Cnd 1	Cnd 2	Cnd 3	Cnd 4	Cnd 5
n	92	120	93	93	115	83	91	81	83	74
Comfortable reasons										
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%
Uncomfortable reasons										
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.

“Decision Strategies and Susceptibly to Phishing”

- Julie Downs, Mandy Holbrook, and Lorrie Faith Cranor
- 2006
- Interviewed 20 normal people about their strategies for identifying phishing emails

“Decision Strategies and Susceptibly to Phishing”

- Julie Downs, Mandy Holbrook, and Lorrie Faith Cranor
- 2006
- Interviewed 20 normal people about their strategies for identifying phishing emails

Quilt and dress containing the most frequently used (i.e. terrible) passwords

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, actual URL www.citibank-accountonline.com
  - Reset password from "Paypal", link "Click here to activate", actual URL 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	% Sensitive	Takeaway
Spoofed “from” address	95%	Good – strange email sources are suspicious
Broken image links on the website	80%	Not good – decent phishing pages will look correct
Strange URL	55%	Good – odd spelling or TLDs are indicative of phishing sites
Awareness of HTTPS	35%	Not good – any website, including phishing sites, can use TLS

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

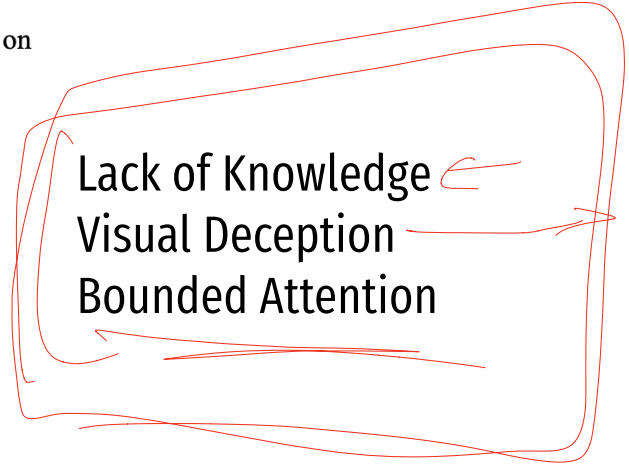
Participants and Overall Results

- 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

- Good phishing websites fooled 90% of participants.
- Existing anti-phishing browsing cues are ineffective. 23% of participants in our study did not look at the address bar, status bar, or the security indicators.
- On average, our participant group made mistakes on our test set 40% of the time.



“Social Phishing”

- Problem: the prior study was conducted in a lab
  - Subjects knew they were participating in an experiment
  - May impact ecological validity of results
    - i.e. would people have behaved differently under real-world circumstances?
- Tom Jagatic, Nathaniel Johnson, Markus Jakobsson, and Filippo Menczer, 2005
  - Sent actual phishing emails to 581 Indiana University undergrads
  - Deception study – students were unaware of the experiment
- **Hugely controversial study**

Methodology

- Students were sent a typical phishing email
  - “Hey, check out this cool link!”
  - Link appeared to point to a university website
  - Actual URL was www.whuffo.com
  - Site asked user to input their university username and password
  - Credentials were checked against the actual university system

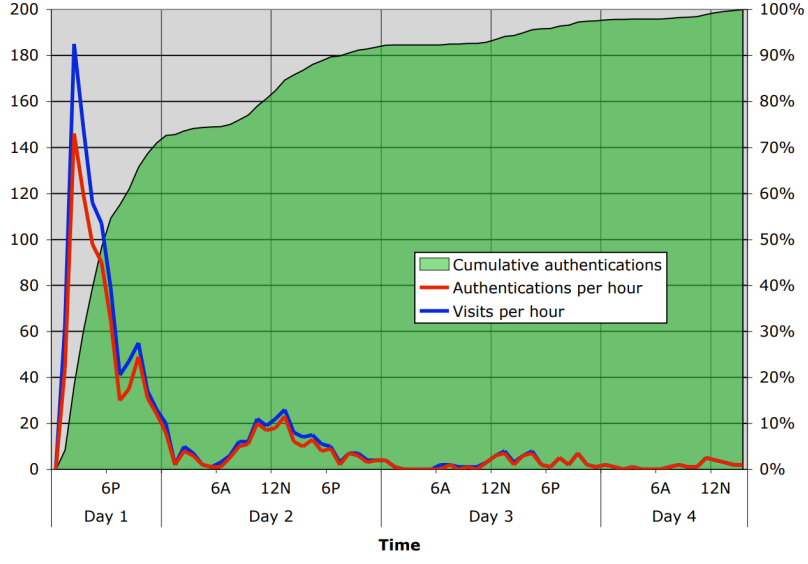
Methodology

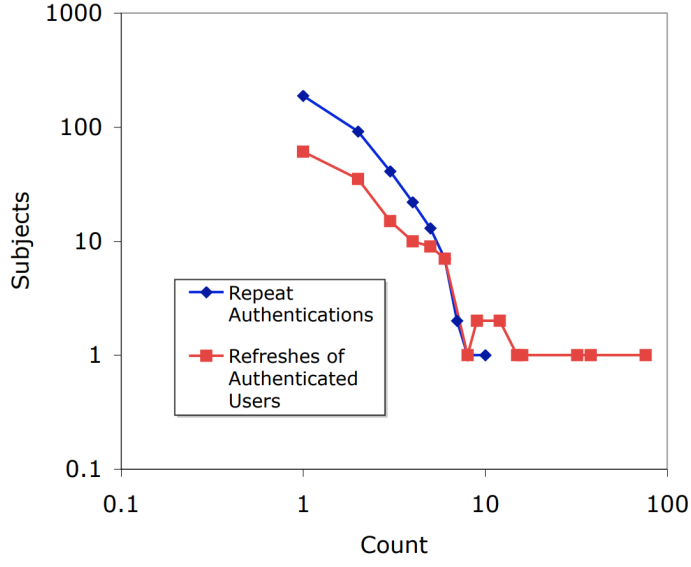
- Students were sent a typical phishing email
  - “Hey, check out this cool link!”
  - Link appeared to point to a university website
  - Actual URL was www.whuffo.com
  - Site asked user to input their university username and password
  - Credentials were checked against the actual university system
- Tested two treatments for email origin
  1. A generic U. of Indiana email address
  2. Spoofed from an actual friend of the victim (scraped from Facebook)

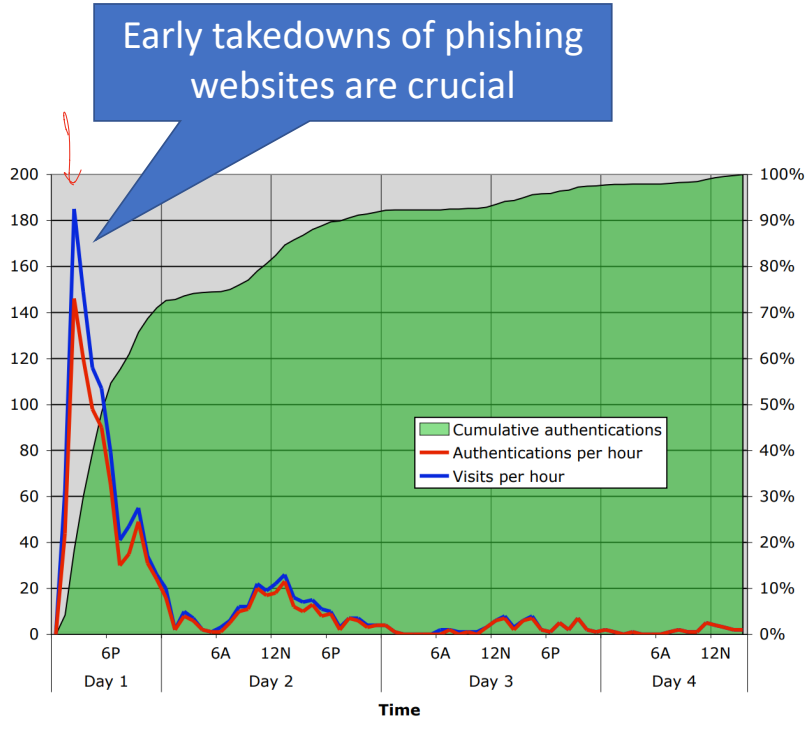
Results

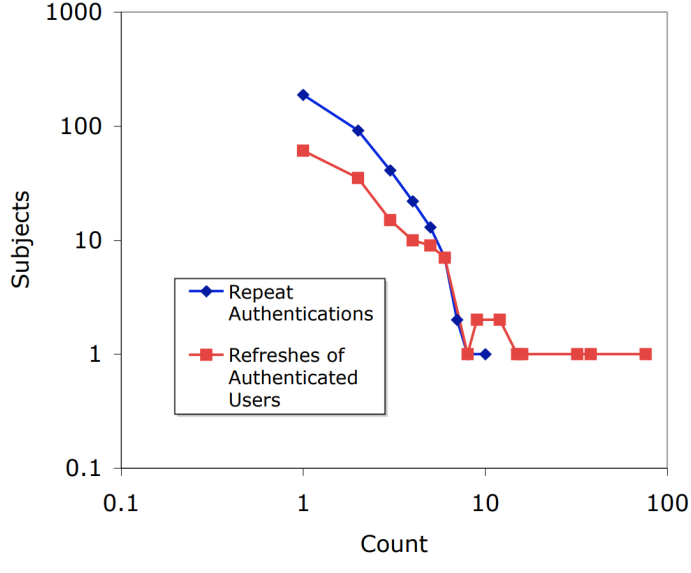
	# of Targeted Students	% Success	95% C.I.
Generic email	94	16%	9-23%
“From a friend”	487	72%	68-76%

- Generic attacks were quite successful
  - Agrees with results from other studies
- Socially augmented attacks were devastatingly effective
  - Friendship information is widely available on the web
  - People do not understand that emails are easy to spoof
- Social attacks were more effective if the “friend” was of the opposite sex

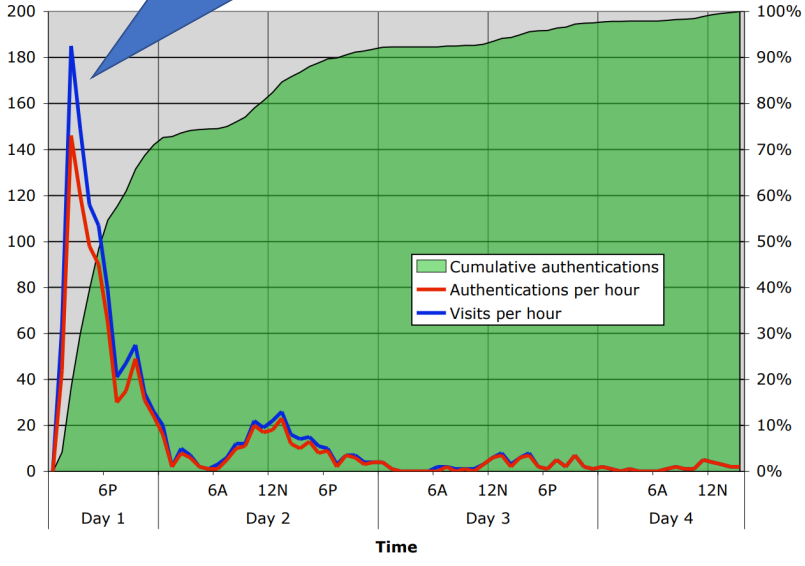

200
180
160
140
120
100
80
60
40
20
0
100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
Cumulative authentications
Authentications per hour
Visits per hour
6P
6A
12N
6P
6A
12N
6P
6A
12N
Day 1
Day 2
Day 3
Day 4
Time

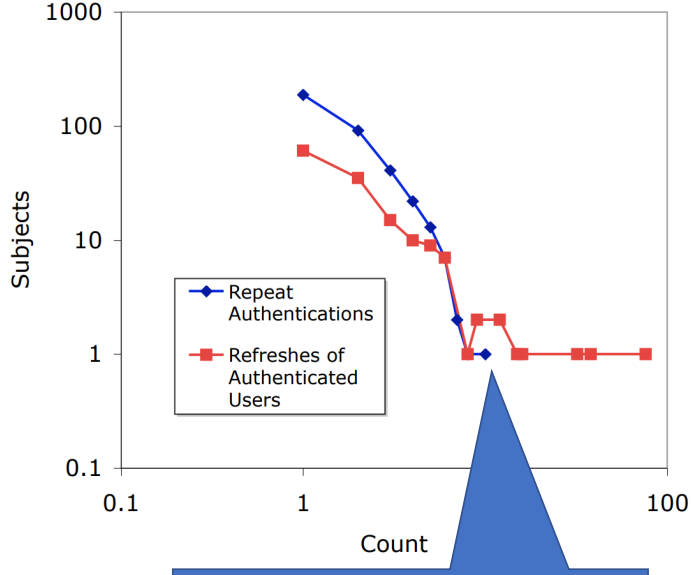

1000
100
10
1
0.1
Subjects
Repeat Authentications
Refreshes of Authenticated Users
0.1
1
10
100
Count


Early takedowns of phishing websites are crucial
200
180
160
140
120
100
80
60
40
20
0
100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
Cumulative authentications
Authentications per hour
Visits per hour
6P
6A
12N
6P
6A
12N
6P
6A
12N
Day 1
Day 2
Day 3
Day 4
Time


1000
100
10
1
0.1
Subjects
Repeat Authentications
Refreshes of Authenticated Users
0.1
1
10
100
Count

Early takedowns of phishing websites are crucial





Some victims visited and logged in multiple times!

Debriefing

Debriefing

- For ethical reasons, deception studies always debrief participants
  - Explain how and why they have been experimented on
  - Give them a chance to ask questions, learn, and just vent
- Study authors set up a forum for participants to leave comments
  - 440 total comments
  - Most comments were supportive of the experiment and the learning experience
  - However, a small number of very vocal complaints

Analysis of Comments

- Anger
  - Called the experiment unethical, inappropriate, illegal, unprofessional, fraudulent, self-serving, and/or useless
  - Called for the researchers to be fired, prosecuted, expelled, or otherwise reprimanded
  - *Demonstrates the psychological toll phishing attacks can have*

Analysis of Comments

- Anger
  - Called the experiment unethical, inappropriate, illegal, unprofessional, fraudulent, self-serving, and/or useless
  - Called for the researchers to be fired, prosecuted, expelled, or otherwise reprimanded
  - *Demonstrates the psychological toll phishing attacks can have*
- Denial
  - Zero comments included an admission of culpability
  - Many complaints were posted “on behalf of friends who were phished”
  - *Many people find it hard to admit their vulnerability*

Analysis of Comments

- Misunderstanding of email
  - Many subjects were convinced the researchers had hacked their inbox
  - *People don’t understand that email spoofing is easy*

Analysis of Comments

- Misunderstanding of email
  - Many subjects were convinced the researchers had hacked their inbox
  - *People don't understand that email spoofing is easy*
- Underestimation of privacy risks
  - Many subjects didn't know how the researchers new their friends
  - Others were mad that public information from their Facebook had been used
  - *People severely underestimate the privacy risks of social networking*

“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	
	1st role play	2nd role play	1st role play	2nd 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	
	1st role play	2nd role play	1st role play	2nd 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

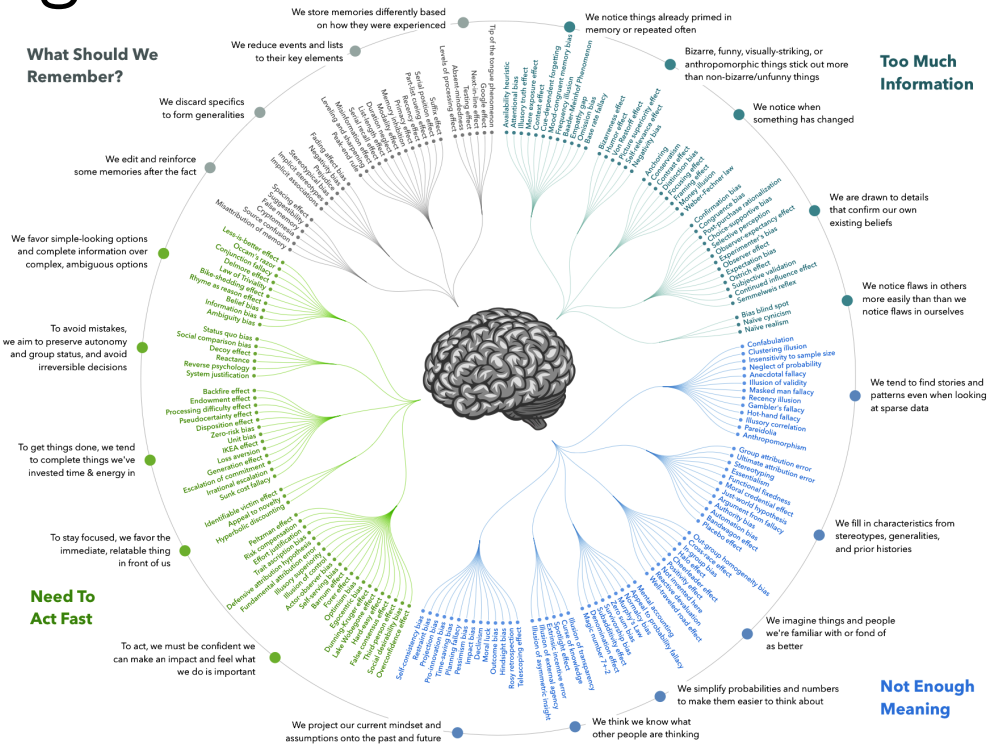
Summary of findings

Prior exposure to phishing education is associated with less susceptibility to phishing, suggesting that phishing education may be an effective tool. Also, more risk-averse participants tended to fall for fewer phish.

Gender and age are two key demographics that predict phishing susceptibility. Specifically, women click on links in phishing emails more often than men do, and also are much more likely than men to continue on to give information to phishing websites. In part, this difference appears to be because women have less technical training and less technical knowledge than men. There is also a

Demographics such as age, gender, race, and education do not affect the amount of learning, suggesting that good training materials can provide benefit for all groups. However, while the 40% reduction in phishing susceptibility after training is substantial, even after training participants fell for 28% of the phishing messages in our roleplay. This finding shows that education is effective and needed but is not a cure-all.

Heuristics —> Cognitive Bias



DESIGNHACKS.CO · CATEGORIZATION BY BUSTER BENSON · ALGORITHMIC DESIGN BY JOHN MANOOGIAN III (JM3) · DATA BY WIKIPEDIA

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

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

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 Girlfrien First Time Dies Fr

633,

Man Girlfrien For Th Time Di E. C

10

631,589

Muslim Figure: "We Must Have Free Menus Or Leave U.S." How You Respond Th

Which biases?

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).

Anchoring effect

Soups 2020 conference

"soups.usenix.org"

"Soups 2020"