ECE750: Usable Security and Privacy

USEC Introduction

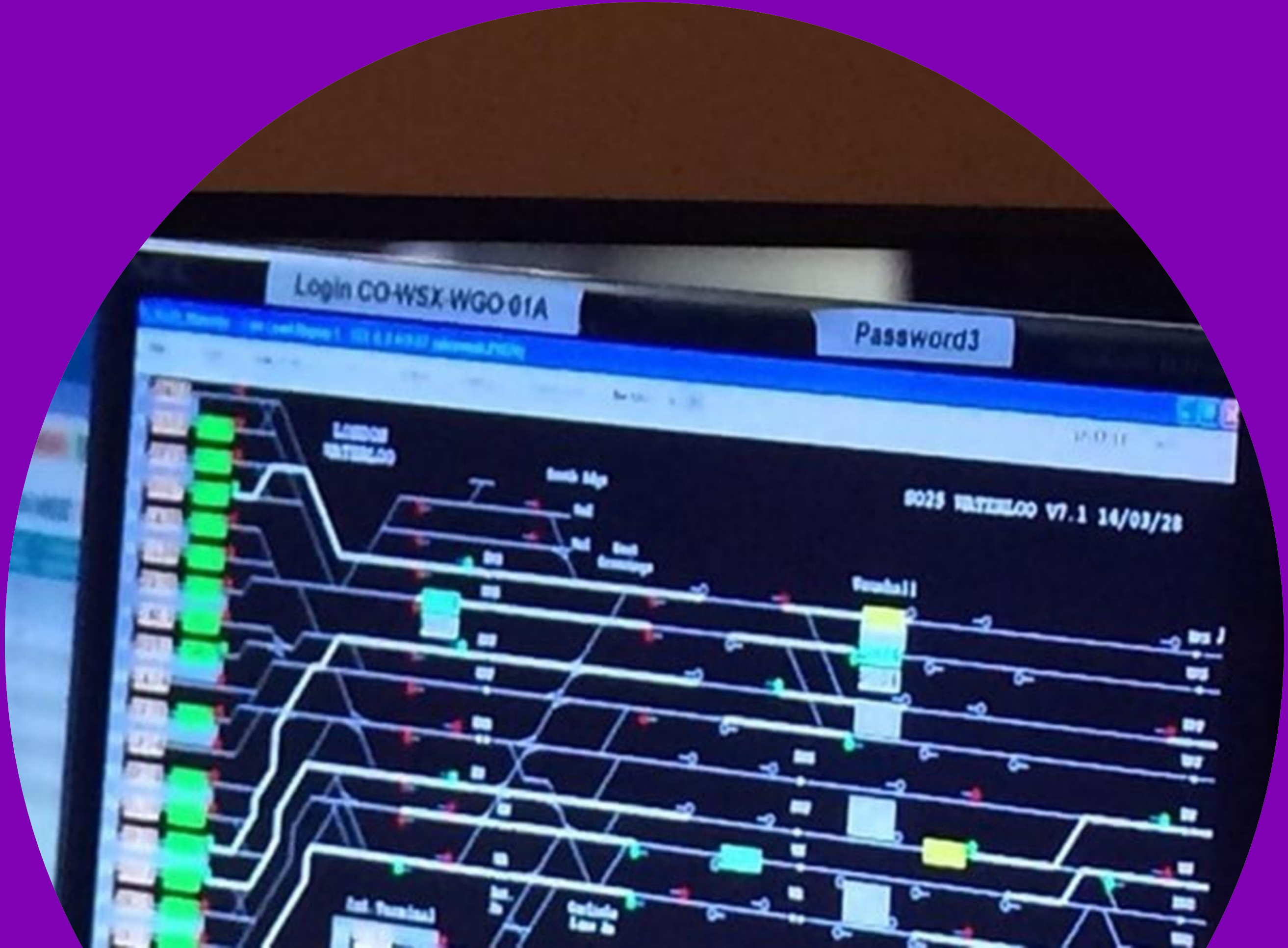
Dr. Kami Vaniea,
Electrical and Computer Engineering
kami.vaniea@uwaterloo.ca

TULiPS
Technology Usability Lab in Privacy and Security

University of Waterloo | Faculty of Engineering

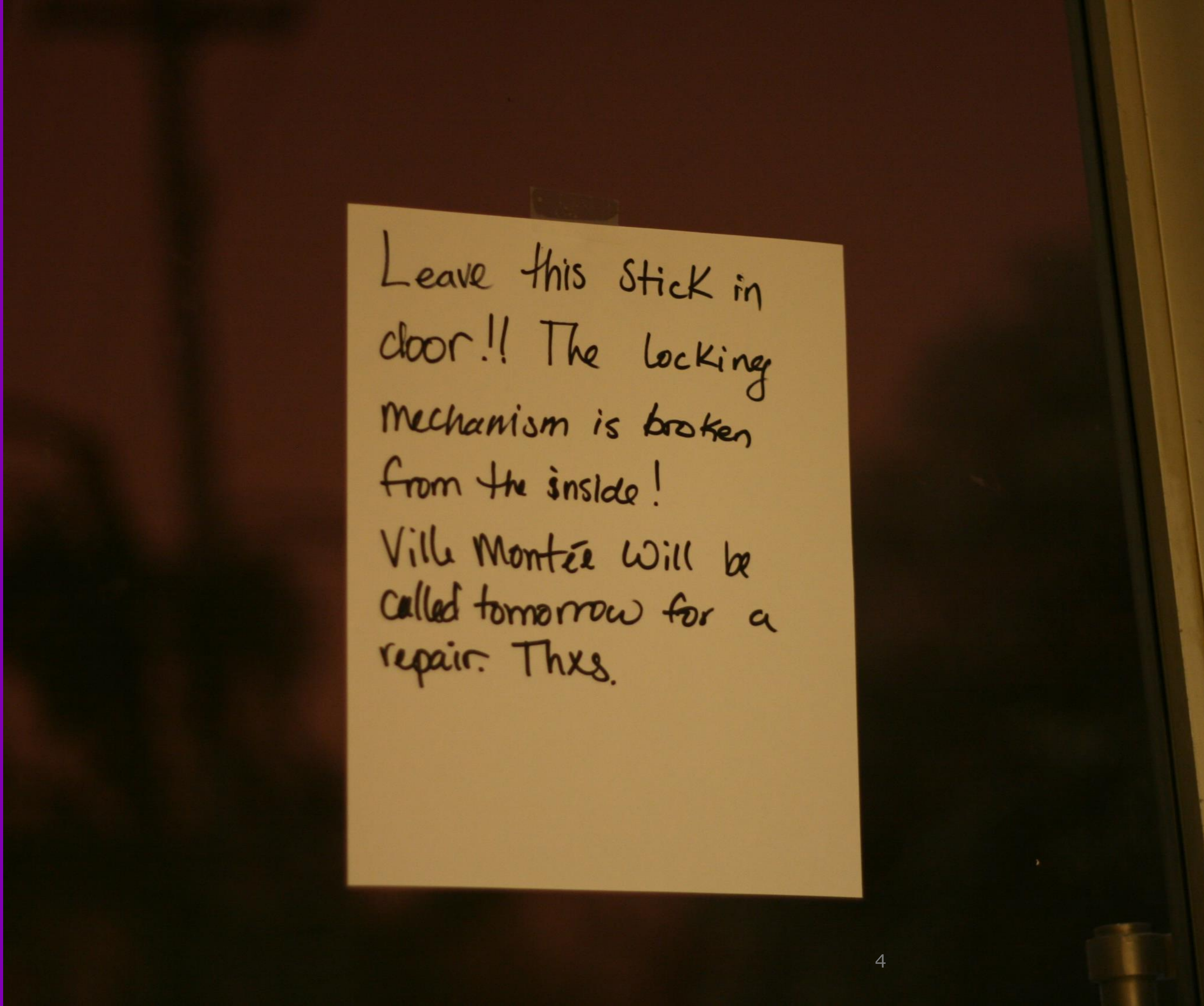
HUMANS AND CONTEXT

Usable Security and Privacy



People handle complex security decisions every day.

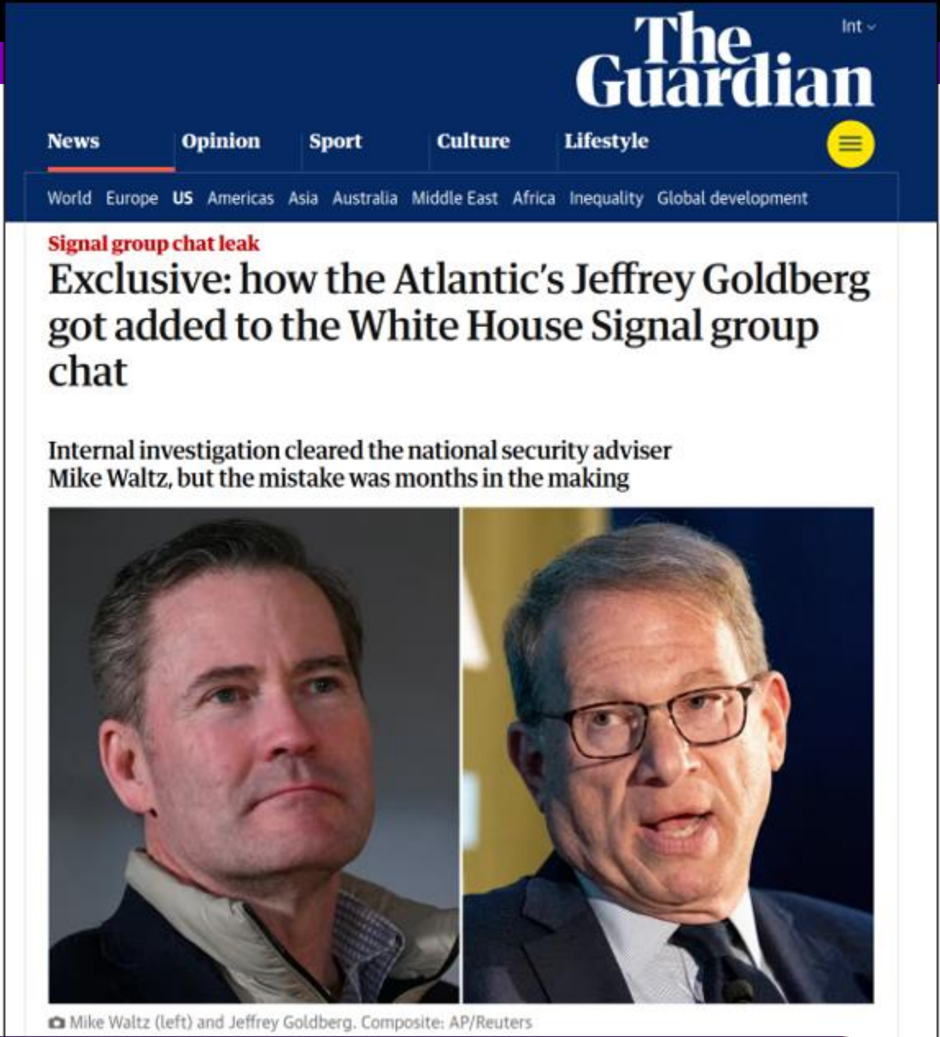
Context strongly impacts how we interpret signs like this one.



Leave this stick in door!! The locking mechanism is broken from the inside!
Ville Montée will be called tomorrow for a repair. Thxs.

Computers are bad at context

- Journalist mistakenly added to a sensitive chat
- Wrong phone number associated with a name in the phone book
- iPhone put it there....



Signal group chat leak

Exclusive: how the Atlantic's Jeffrey Goldberg got added to the White House Signal group chat

Internal investigation cleared the national security adviser Mike Waltz, but the mistake was months in the making

Mike Waltz (left) and Jeffrey Goldberg. Composite: AP/Reuters

"According to the White House, the number was erroneously saved during a "contact suggestion update" by Waltz's iPhone, which one person described as the function where an iPhone algorithm adds a previously unknown number to an existing contact that it detects may be related."

that started during the 2024 campaign and went unnoticed until Waltz created the group chat last month.

The “Citizens Bank” problem

I bank at Citizens Bank

Citizens®	https://www.citizensbank.com
CITIZENS BANK	https://www.citizensebank.com/
Citizens Bank & Trust	https://www.citizens-bank.com
csb Citizens State Bank Member FDIC FDIC-Insured - Backed by the full faith and credit of the U.S. Government	https://www.citizensbank.net
CITIZENS BANK & TRUST CO	https://www.ctznsbank.com

The "Citizens Bank" problem

I bank at Citizens Bank

FirstCitizensBank

https://www.firstcitizens.com/

https://www.citizensfb.com/

CITIZENS FIRST BANK

THE CITIZENS BANK COMPANY

https://my.thecitizens.com

https://www.gocitizensbank.com

CITIZENS BANK Est. 1904

CITIZENS ALLIANCE BANK

Customer Driven. Community Focused.®

https://www.citizensalliancebank.com/

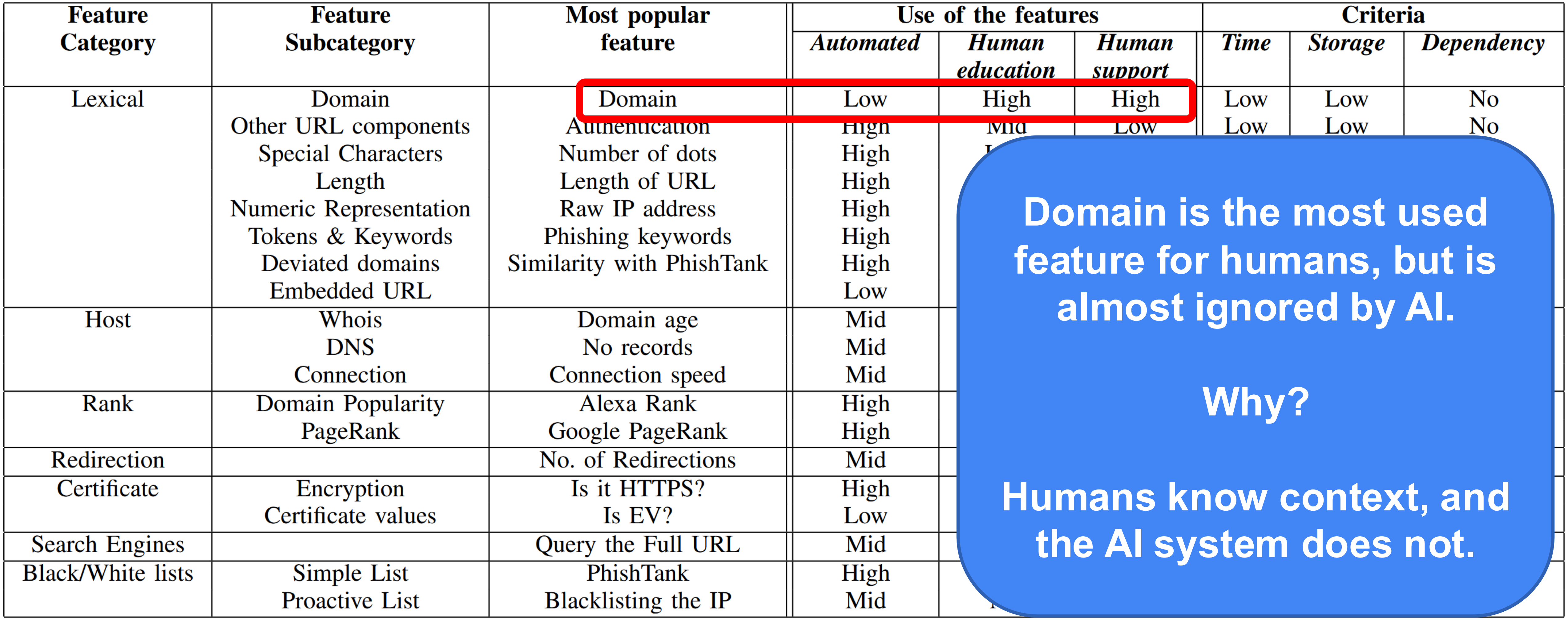
https://www.citizensbankwi.bank

citizens bank

CITIZENS BUSINESS BANK

https://www.cbbank.com/

Human- and AI-facing URL features



Feature Category	Feature Subcategory	Most popular feature	Use of the features			Criteria		
			Automated	*Human education*	*Human support*	*Time*	*Storage*	*Dependency*
Lexical	Domain	Domain	Low	High	High	Low	Low	No
	Other URL components	Authentication	High	Mid	Low	Low	Low	No
	Special Characters	Number of dots	High					
	Length	Length of URL	High					
	Numeric Representation	Raw IP address	High					
	Tokens & Keywords	Phishing keywords	High					
	Deviated domains	Similarity with PhishTank	High					
	Embedded URL		Low					
Host	Whois	Domain age	Mid					
	DNS	No records	Mid					
	Connection	Connection speed	Mid					
Rank	Domain Popularity	Alexa Rank	High					
	PageRank	Google PageRank	High					
Redirection		No. of Redirections	Mid					
Certificate	Encryption	Is it HTTPS?	High					
	Certificate values	Is EV?	Low					
Search Engines		Query the Full URL	Mid					
Black/White lists	Simple List	PhishTank	High					
	Proactive List	Blacklisting the IP	Mid					

Domain is the most used feature for humans, but is almost ignored by AI.

Why?

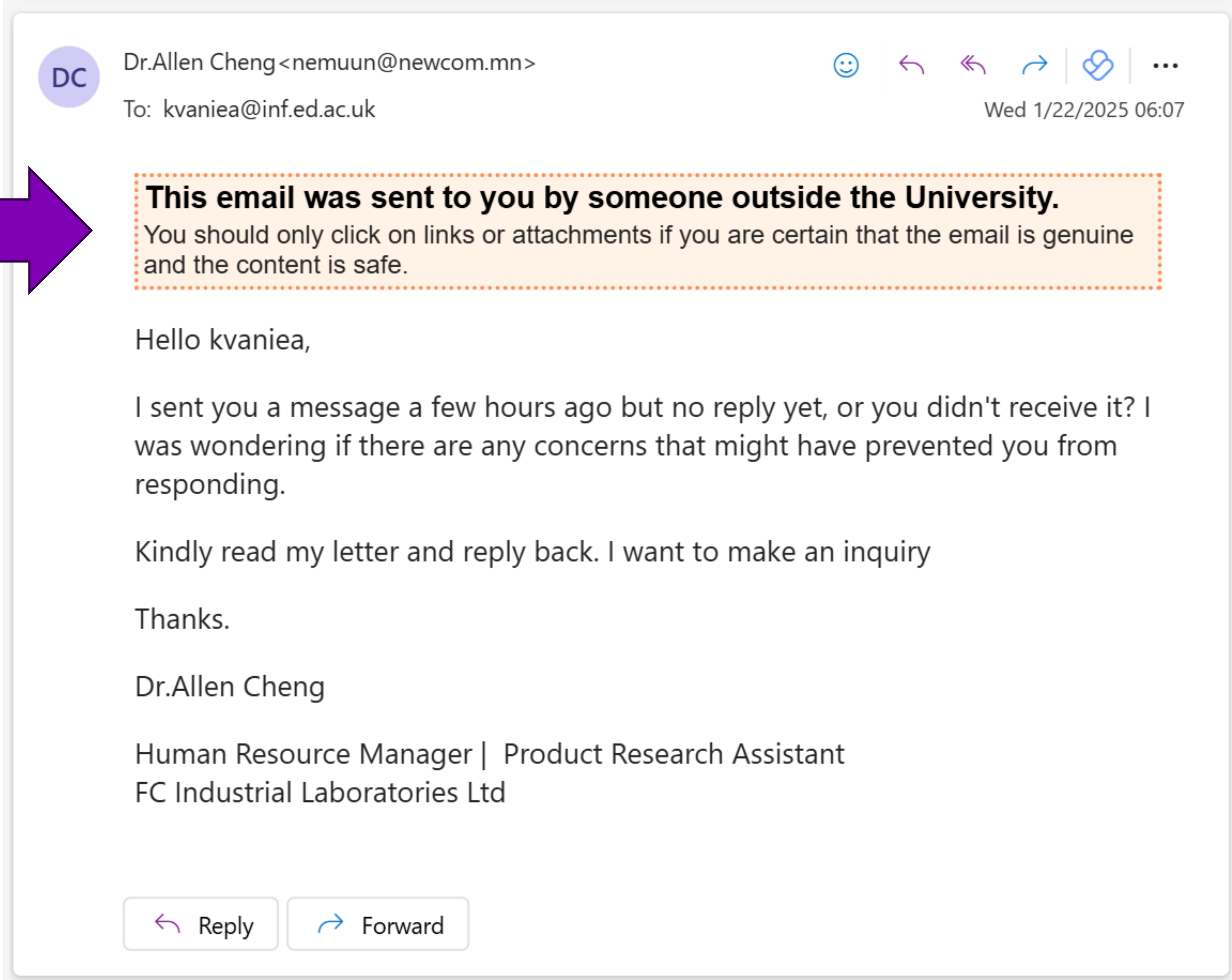
Humans know context, and the AI system does not.

K. Althobaiti, G. Rummani, K. Vaniea (2019). A Review of Human-and Computer-Facing URL Phishing Features. In IEEE European Symposium on Security and Privacy Workshops (EuroSPW)

Users are told to determine safety:

“only click on links … if you are certain … the content is safe.”

"Safe" is defined as "going where you expect."



Dr.Allen Cheng<nemuun@newcom.mn>

To: kvaniea@inf.ed.ac.uk

Wed 1/22/2025 06:07

This email was sent to you by someone outside the University.
You should only click on links or attachments if you are certain that the email is genuine and the content is safe.

Hello kvaniea,

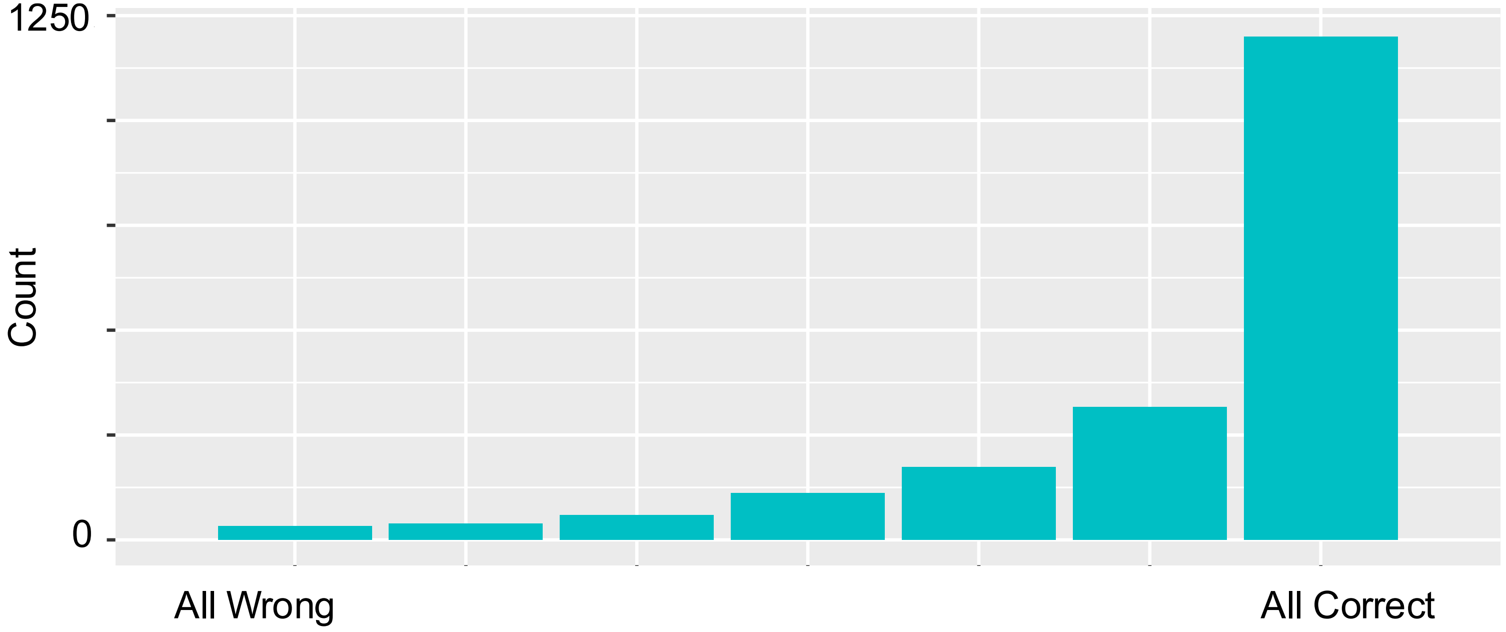
I sent you a message a few hours ago but no reply yet, or you didn't receive it? I was wondering if there are any concerns that might have prevented you from responding.

Kindly read my letter and reply back. I want to make an inquiry

Thanks.

Dr.Allen Cheng

Human Resource Manager | Product Research Assistant
FC Industrial Laboratories Ltd



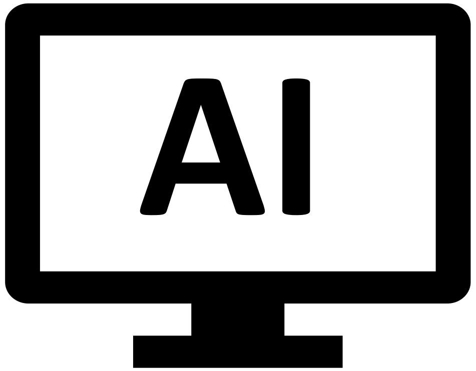
Name in domain

profile.**facebook**.com

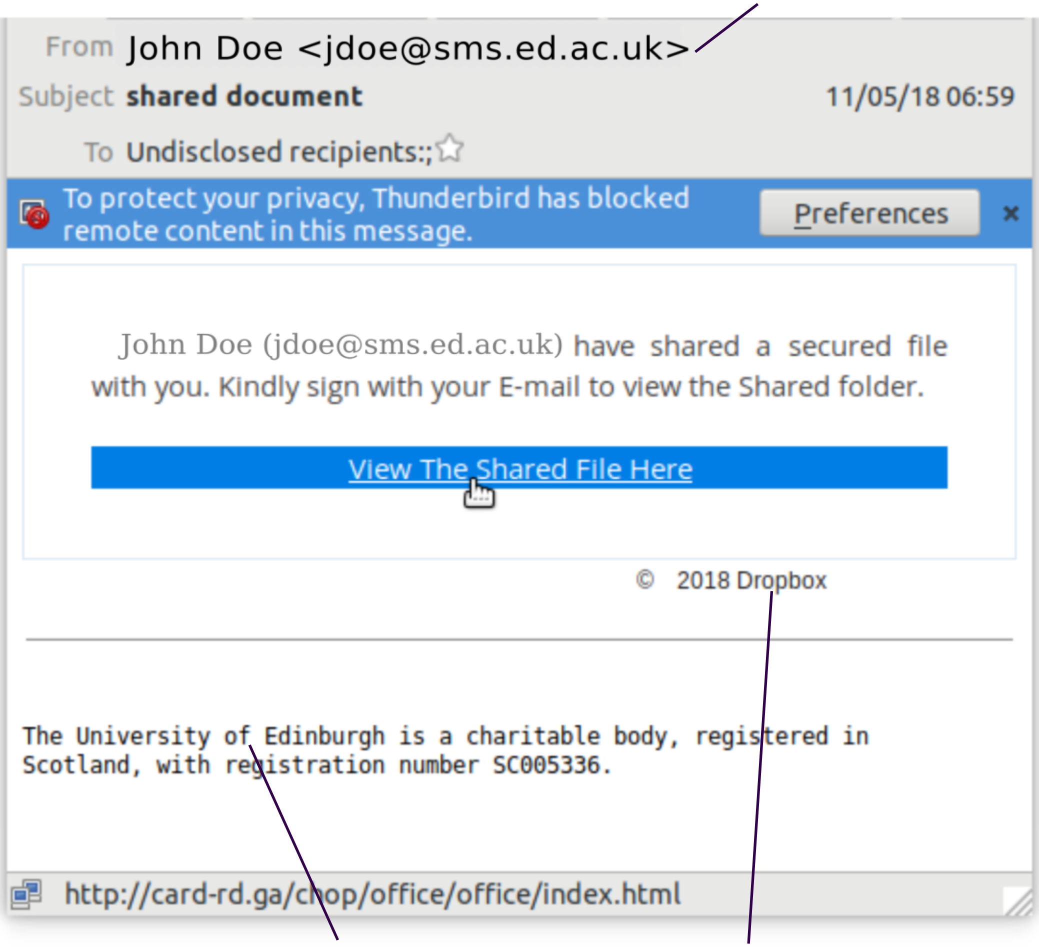
mobile.**paypal**.com

S.S. Albakry, K. Vaniea, M.K. Wolters; "What is this URL's Destination? Empirical Evaluation of Users' URL Reading"; In CHI 2020.

Who is the email claiming to be from?



University email address



From John Doe <jdoe@sms.ed.ac.uk>

Subject **shared document** 11/05/18 06:59

To Undisclosed recipients:; ☆

To protect your privacy, Thunderbird has blocked remote content in this message.

John Doe (jdoe@sms.ed.ac.uk) have shared a secured file with you. Kindly sign with your E-mail to view the Shared folder.

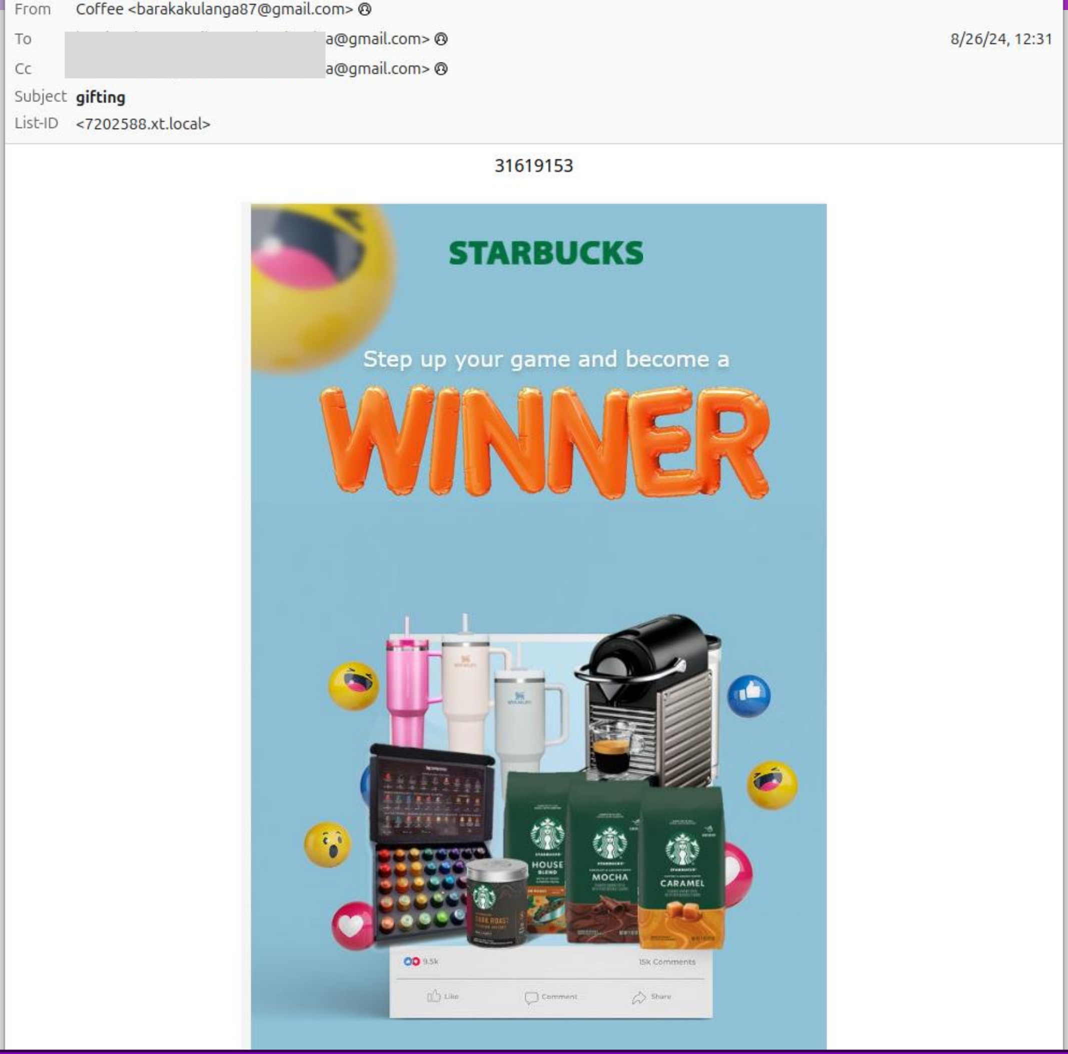
© 2018 Dropbox

The University of Edinburgh is a charitable body, registered in Scotland, with registration number SC005336.

http://card-rd.ga/chop/office/office/index.html

University is named

Image



From Coffee <barakakulanga87@gmail.com>

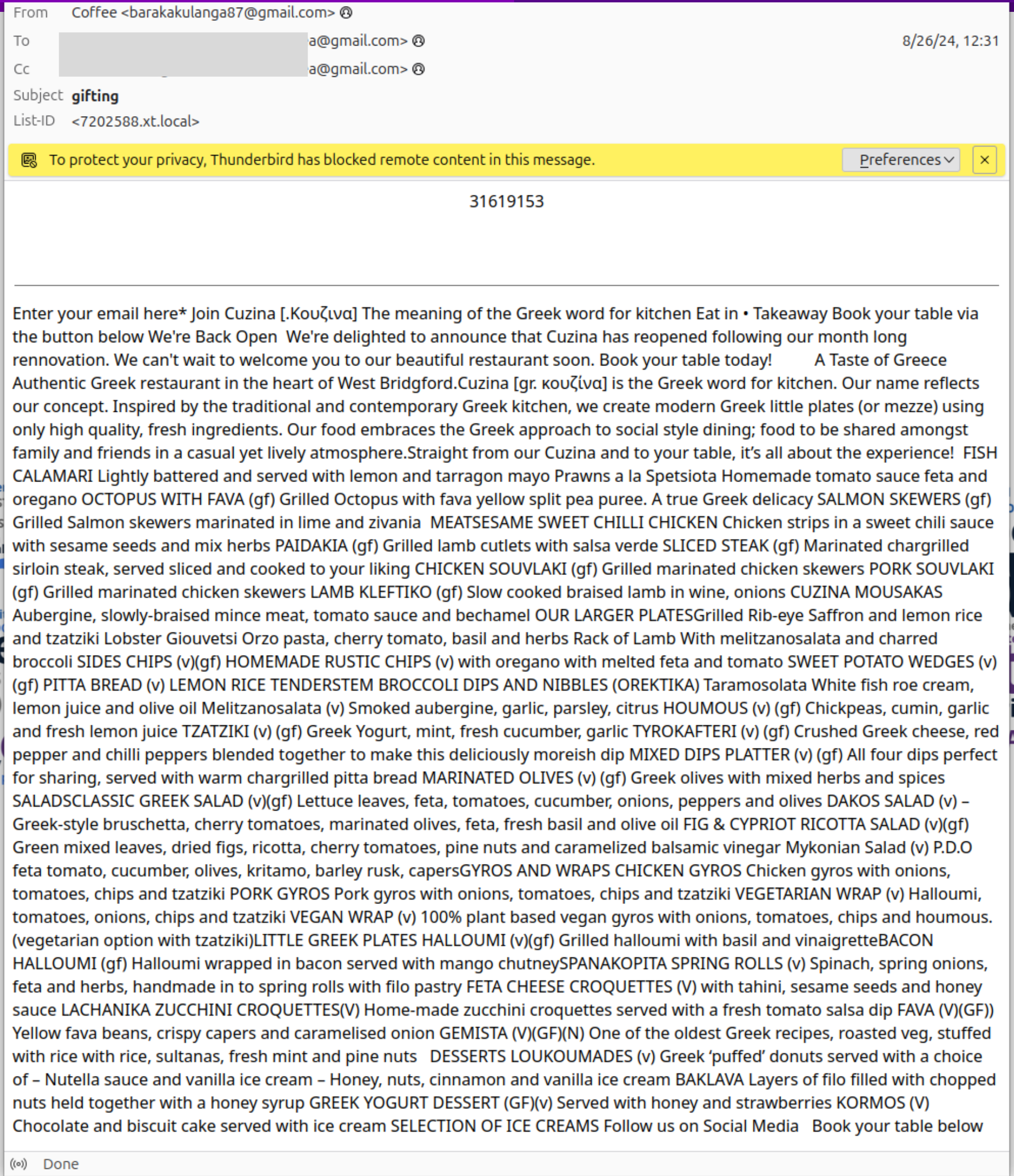
To [redacted]a@gmail.com> 8/26/24, 12:31

Cc [redacted]a@gmail.com>

Subject gifting

List-ID <7202588.xt.local>

31619153



From Coffee <barakakulanga87@gmail.com>

To [redacted]a@gmail.com> 8/26/24, 12:31

Cc [redacted]a@gmail.com>

Subject gifting

List-ID <7202588.xt.local>

To protect your privacy, Thunderbird has blocked remote content in this message.

31619153

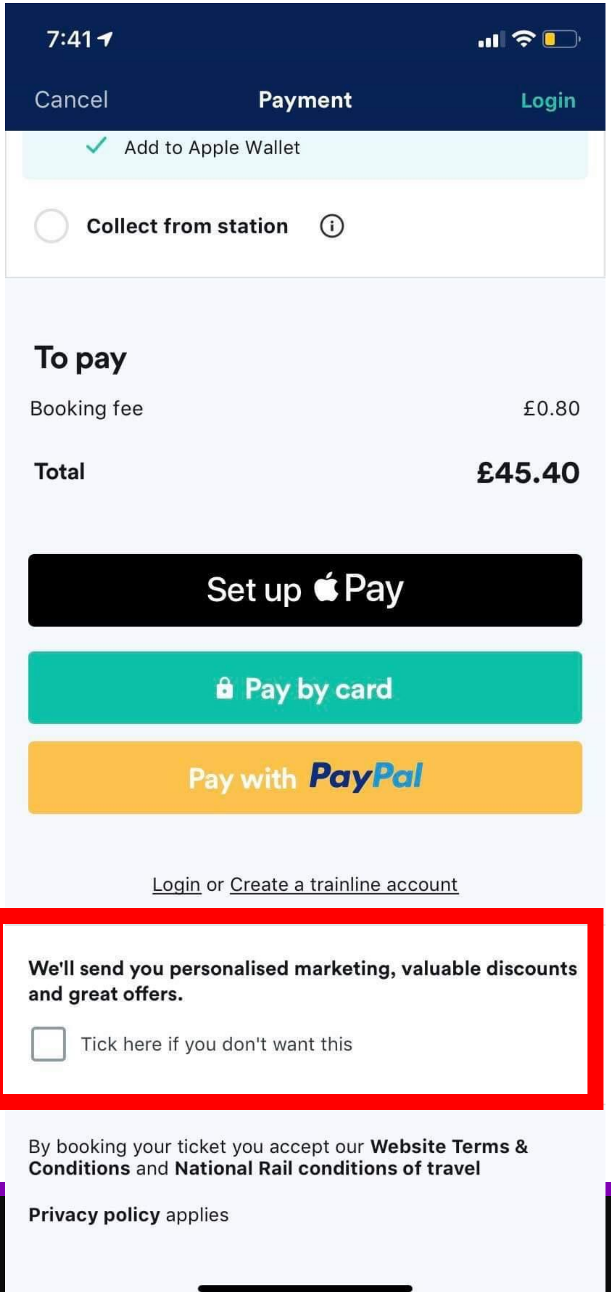
Enter your email here* Join Cuzina [.Κουζινα] The meaning of the Greek word for kitchen Eat in • Takeaway Book your table via the button below We're Back Open We're delighted to announce that Cuzina has reopened following our month long rennovation. We can't wait to welcome you to our beautiful restaurant soon. Book your table today! A Taste of Greece Authentic Greek restaurant in the heart of West Bridgford.Cuzina [gr. κουζίνα] is the Greek word for kitchen. Our name reflects our concept. Inspired by the traditional and contemporary Greek kitchen, we create modern Greek little plates (or mezze) using only high quality, fresh ingredients. Our food embraces the Greek approach to social style dining; food to be shared amongst family and friends in a casual yet lively atmosphere.Straight from our Cuzina and to your table, it's all about the experience! FISH CALAMARI Lightly battered and served with lemon and tarragon mayo Prawns a la Spetsiota Homemade tomato sauce feta and oregano OCTOPUS WITH FAVA (gf) Grilled Octopus with fava yellow split pea puree. A true Greek delicacy SALMON SKEWERS (gf) Grilled Salmon skewers marinated in lime and zivania MEATSESAME SWEET CHILLI CHICKEN Chicken strips in a sweet chili sauce with sesame seeds and mix herbs PAIDAKIA (gf) Grilled lamb cutlets with salsa verde SLICED STEAK (gf) Marinated chargrilled sirloin steak, served sliced and cooked to your liking CHICKEN SOUVLAKI (gf) Grilled marinated chicken skewers PORK SOUVLAKI (gf) Grilled marinated chicken skewers LAMB KLEFTIKO (gf) Slow cooked braised lamb in wine, onions CUZINA MOUSAKAS Aubergine, slowly-braised mince meat, tomato sauce and bechamel OUR LARGER PLATESGrilled Rib-eye Saffron and lemon rice and tzatziki Lobster Giouvetsi Orzo pasta, cherry tomato, basil and herbs Rack of Lamb With melitzanosalata and charred broccoli SIDES CHIPS (v)(gf) HOMEMADE RUSTIC CHIPS (v) with oregano with melted feta and tomato SWEET POTATO WEDGES (v)(gf) PITTA BREAD (v) LEMON RICE TENDERSTEM BROCCOLI DIPS AND NIBBLES (OREKTIKA) Taramosolata White fish roe cream, lemon juice and olive oil Melitzanosalata (v) Smoked aubergine, garlic, parsley, citrus HOUMOUS (v) (gf) Chickpeas, cumin, garlic and fresh lemon juice TZATZIKI (v) (gf) Greek Yogurt, mint, fresh cucumber, garlic TYROKAFTERI (v) (gf) Crushed Greek cheese, red pepper and chilli peppers blended together to make this deliciously moreish dip MIXED DIPS PLATTER (v) (gf) All four dips perfect for sharing, served with warm chargrilled pitta bread MARINATED OLIVES (v) (gf) Greek olives with mixed herbs and spices SALADSCLASSIC GREEK SALAD (v)(gf) Lettuce leaves, feta, tomatoes, cucumber, onions, peppers and olives DAKOS SALAD (v) – Greek-style bruschetta, cherry tomatoes, marinated olives, feta, fresh basil and olive oil FIG & CYPRIOT RICOTTA SALAD (v)(gf) Green mixed leaves, dried figs, ricotta, cherry tomatoes, pine nuts and caramelized balsamic vinegar Mykonian Salad (v) P.D.O feta tomato, cucumber, olives, kritamo, barley rusk, capersGYROS AND WRAPS CHICKEN GYROS Chicken gyros with onions, tomatoes, chips and tzatziki PORK GYROS Pork gyros with onions, tomatoes, chips and tzatziki VEGETARIAN WRAP (v) Halloumi, tomatoes, onions, chips and tzatziki VEGAN WRAP (v) 100% plant based vegan gyros with onions, tomatoes, chips and houmous. (vegetarian option with tzatziki)LITTLE GREEK PLATES HALLOUMI (v)(gf) Grilled halloumi with basil and vinaigretteBACON HALLOUMI (gf) Halloumi wrapped in bacon served with mango chutneySPANAKOPITA SPRING ROLLS (v) Spinach, spring onions, feta and herbs, handmade in to spring rolls with filo pastry FETA CHEESE CROQUETTES (V) with tahini, sesame seeds and honey sauce LACHANIKA ZUCCHINI CROQUETTES(V) Home-made zucchini croquettes served with a fresh tomato salsa dip FAVA (V)(GF)) Yellow fava beans, crispy capers and caramelised onion GEMISTA (V)(GF)(N) One of the oldest Greek recipes, roasted veg, stuffed with rice with rice, sultanas, fresh mint and pine nuts DESSERTS LOUKOUMADES (v) Greek 'puffed' donuts served with a choice of – Nutella sauce and vanilla ice cream – Honey, nuts, cinnamon and vanilla ice cream BAKLAVA Layers of filo filled with chopped nuts held together with a honey syrup GREEK YOGURT DESSERT (GF)(v) Served with honey and strawberries KORMOS (V) Chocolate and biscuit cake served with ice cream SELECTION OF ICE CREAMS Follow us on Social Media Book your table below

Done

https://storage.**googleapis.com**/76c157707
5dba36f1594/64bbeccd27bd2eeaef407ae9d...

Tarini Saka, Kami Vaniea, Nadin Kökciyan (2024). PhishCoder: Efficient Extraction of Contextual Information from Phishing Emails. In Proceedings of the Workshop on Security and Artificial Intelligence (SECAI 2024)

USA Phone



7:41

Cancel **Payment** Login

✓ Add to Apple Wallet

○ **Collect from station** ⓘ

To pay

Booking fee	£0.80
Total	**£45.40**

Set up Pay

🔒 Pay by card

Pay with PayPal

Login or Create a trainline account

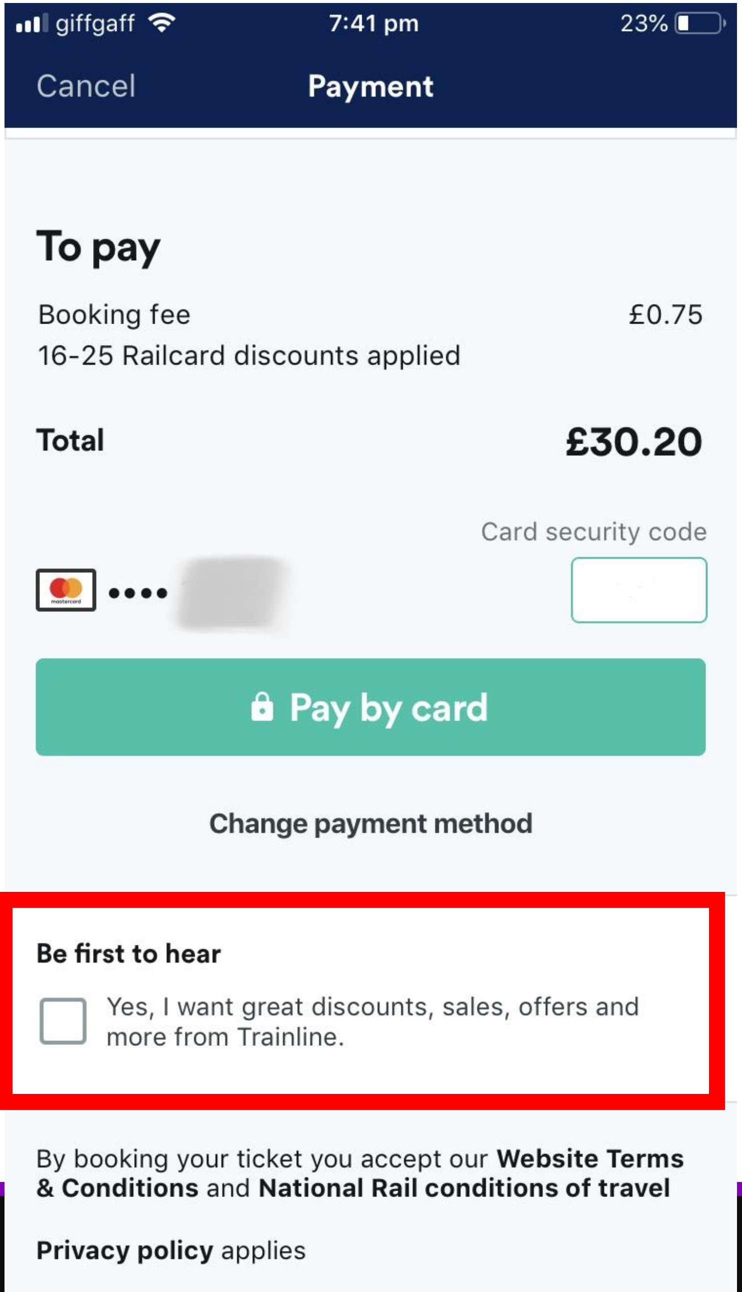
We'll send you personalised marketing, valuable discounts and great offers.

□ Tick here if you don't want this

By booking your ticket you accept our **Website Terms & Conditions** and **National Rail conditions of travel**

Privacy policy applies

EU Phone



giffgaff 7:41 pm 23%

Cancel **Payment**

To pay

Booking fee	£0.75
16-25 Railcard discounts applied	
Total	**£30.20**

Card security code

•••• [redacted]

🔒 Pay by card

Change payment method

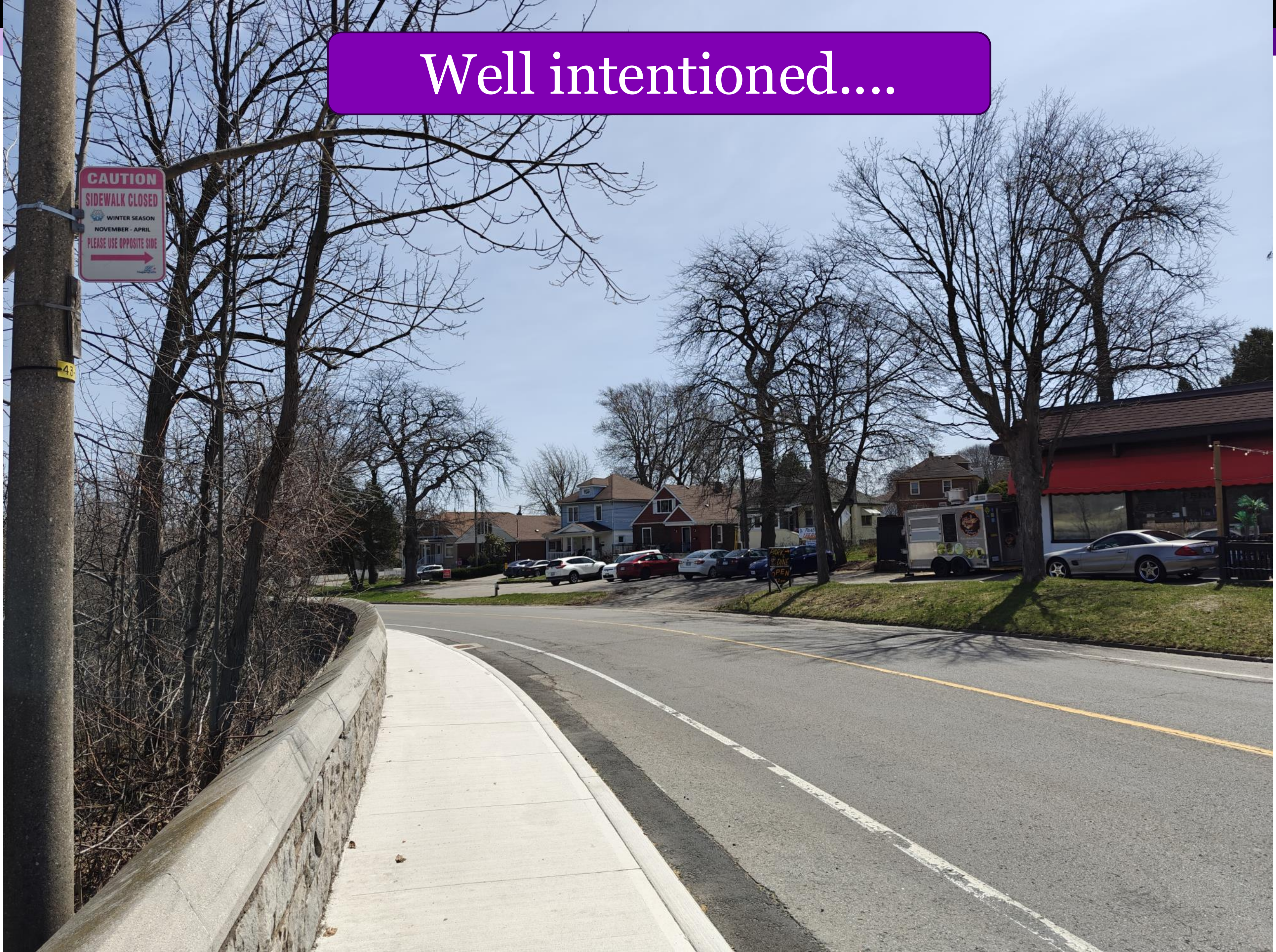
Be first to hear

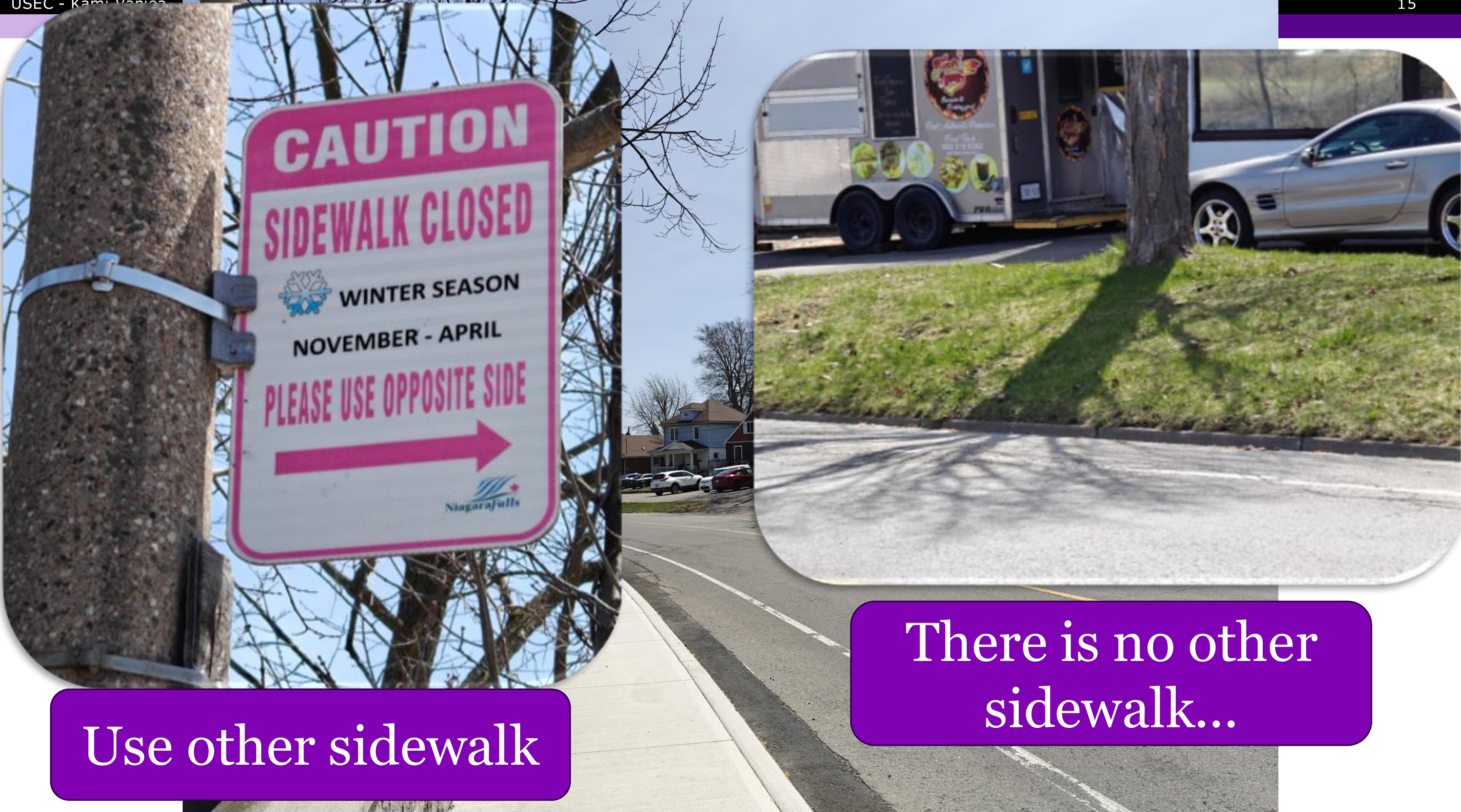
□ Yes, I want great discounts, sales, offers and more from Trainline.

By booking your ticket you accept our **Website Terms & Conditions** and **National Rail conditions of travel**

Privacy policy applies

Well intentioned….





Use other sidewalk

There is no other sidewalk...

WHAT IS USABLE SECURITY AND PRIVACY?

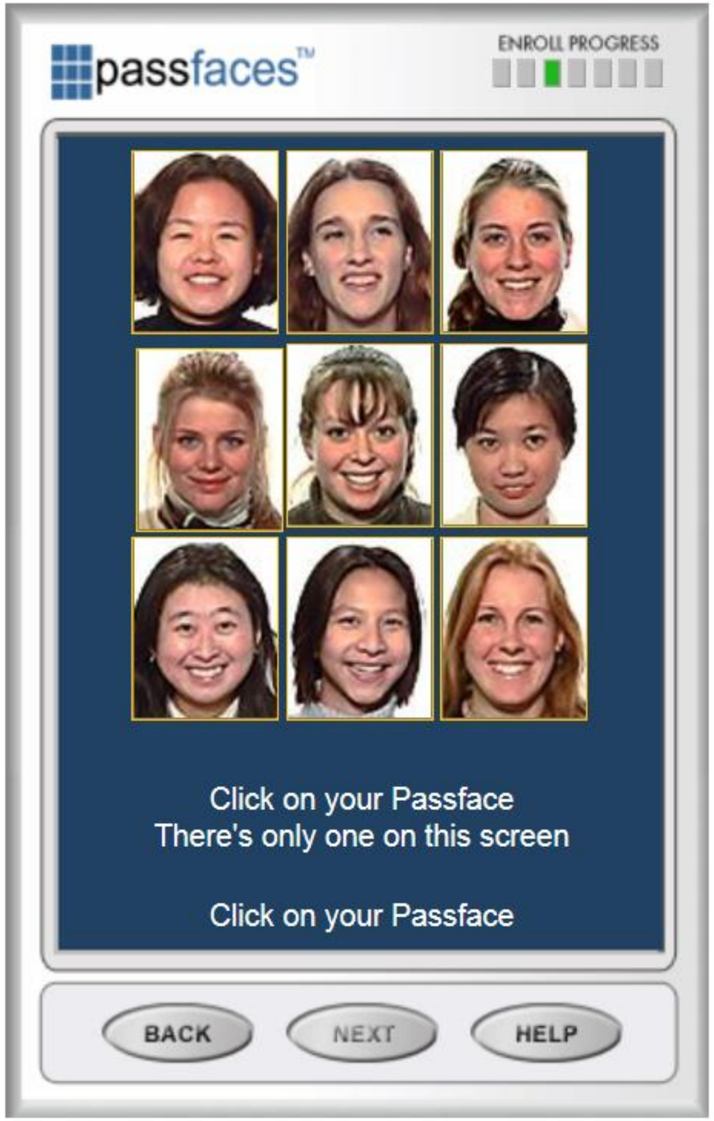
Security and usability together

Security	Usability/HCI	Usable Security and Privacy
Humans are a secondary constraint to security constraints	Humans are the primary constraint, security rarely considered	Human factors and security are both primary constraints
Humans considered primarily in their role as adversaries/attackers	Concerned about human error but not human attackers	Concerned about both normal users and adversaries
Involves threat models	Involves task models, mental models, cognitive models	Involves threat models AND task models, mental models, etc.
Focus on security metrics	Focus on usability metrics	Considers usability and security metrics together
User studies rarely done	User studies common	User studies common, often involve deception + active adversary

Based on slides by Lorrie Cranor

PassFaces

- Users have a set of faces instead of a set of numbers/letters as their password
- Humans are better at recognizing things than they are at recalling information
- High feature information, like faces, are theoretically easier to recognize

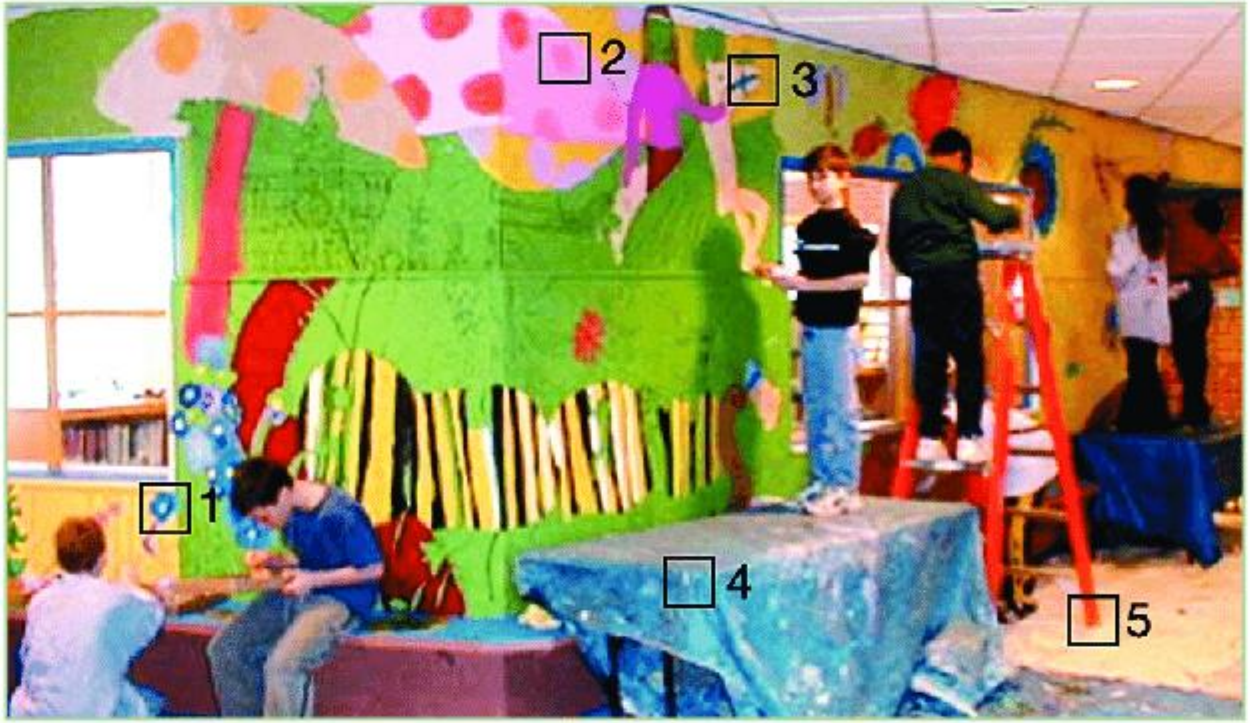


Click on your Passface
There's only one on this screen

Click on your Passface

Graphical Passwords

Users select 5 points on the image in order.



Wiedenbeck, Waters, Birget, Brodskiy, and Memon; "Authentication Using Graphical Passwords: Effects of Tolerance and Image Choice"

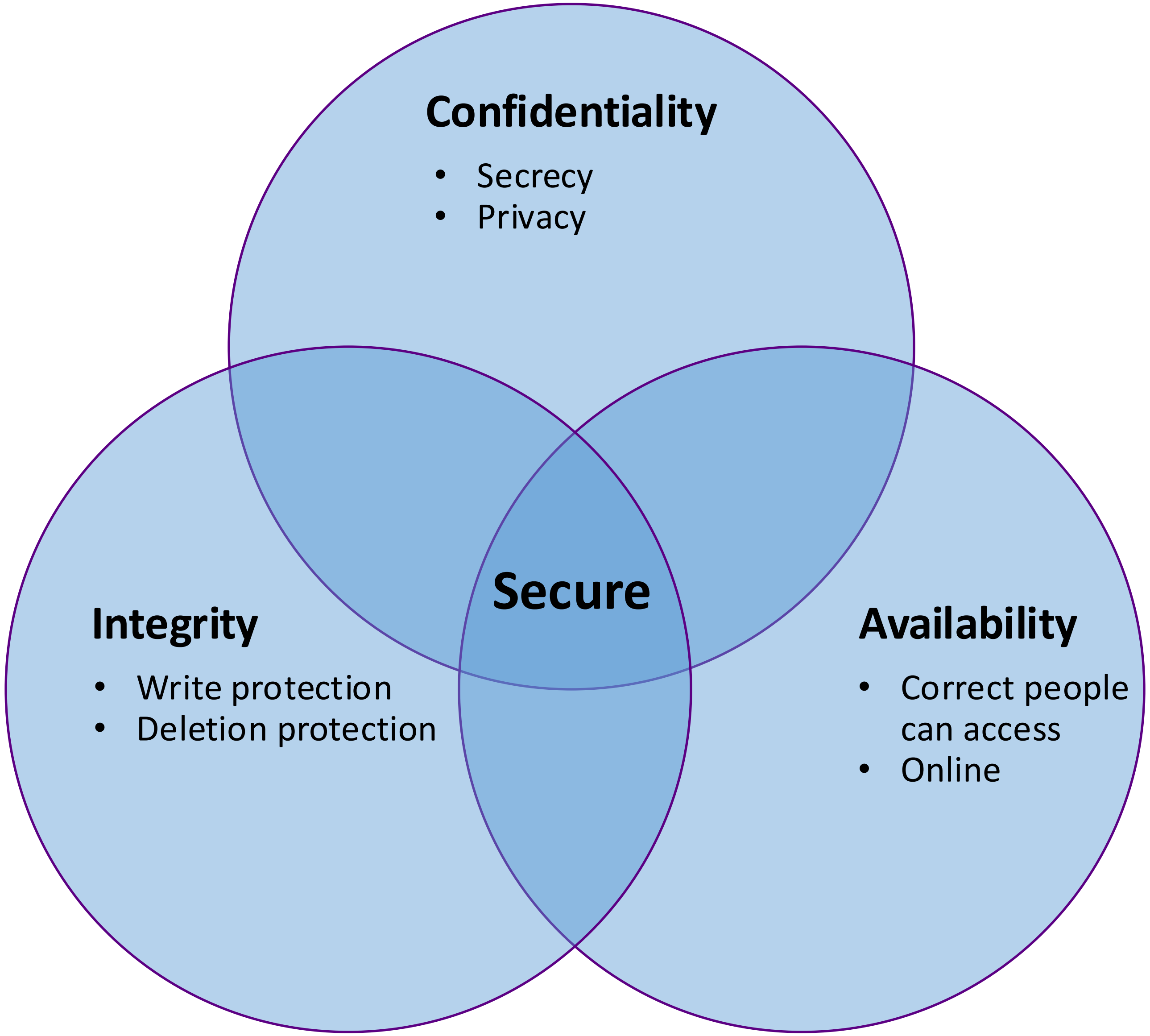
User-selected graphical passwords

Security	Usability/HCI	Usable Security and Privacy
What is the space of possible passwords? How can we make the password space larger to make the password harder to guess? How are the stored passwords secured? Can an attacker gain knowledge by observing a user entering their password?	How difficult is it for a user to create, remember, and enter a graphical password? How long does it take? How hard is it for users to learn the system? Are users motivated to put in effort to create good passwords? Is the system accessible using a variety of devices, for users with disabilities?	All the security/privacy and usability HCI questions How do users select graphical passwords? How can we help them choose passwords harder for attackers to predict? As the password space increases, what are the impacts on usability factors and predictability of human selection?

Based on slides by Lorrie Cranor

Defining Security

- Confidentiality
  - Ensures that computer-related assets are accessed only by authorized parties.
- Integrity
  - Assets can be modified only by authorized parties or only in authorized ways.
- Availability
  - Assets are accessible to authorized parties at appropriate times.

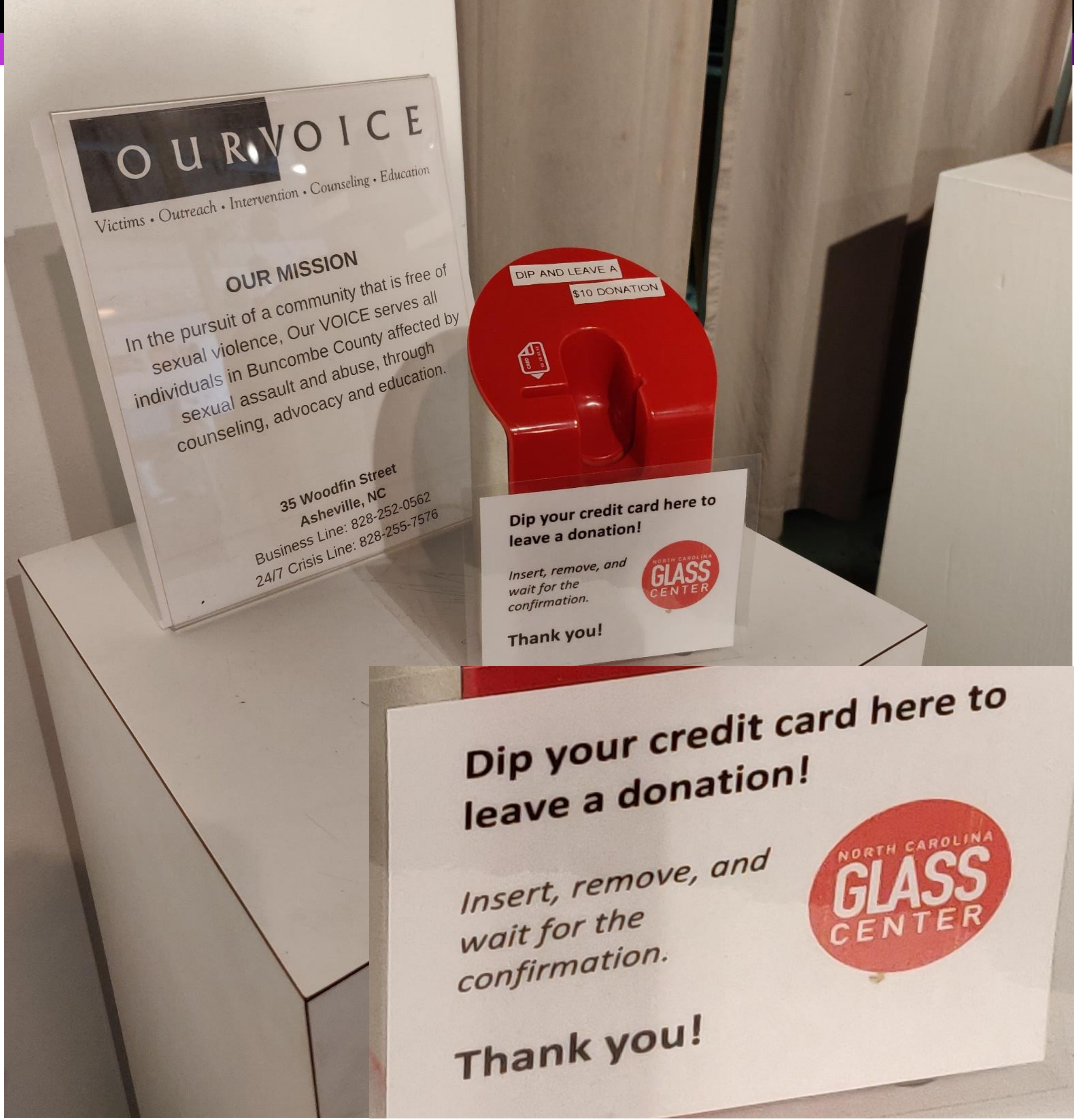


Security properties to ensure

Confidentiality	No improper information gathering
Integrity	Data has not been (maliciously) altered
Availability	Data/services can be accessed as desired
Accountability	Actions are traceable to those responsible
Authentication	User or data origin accurately identifiable

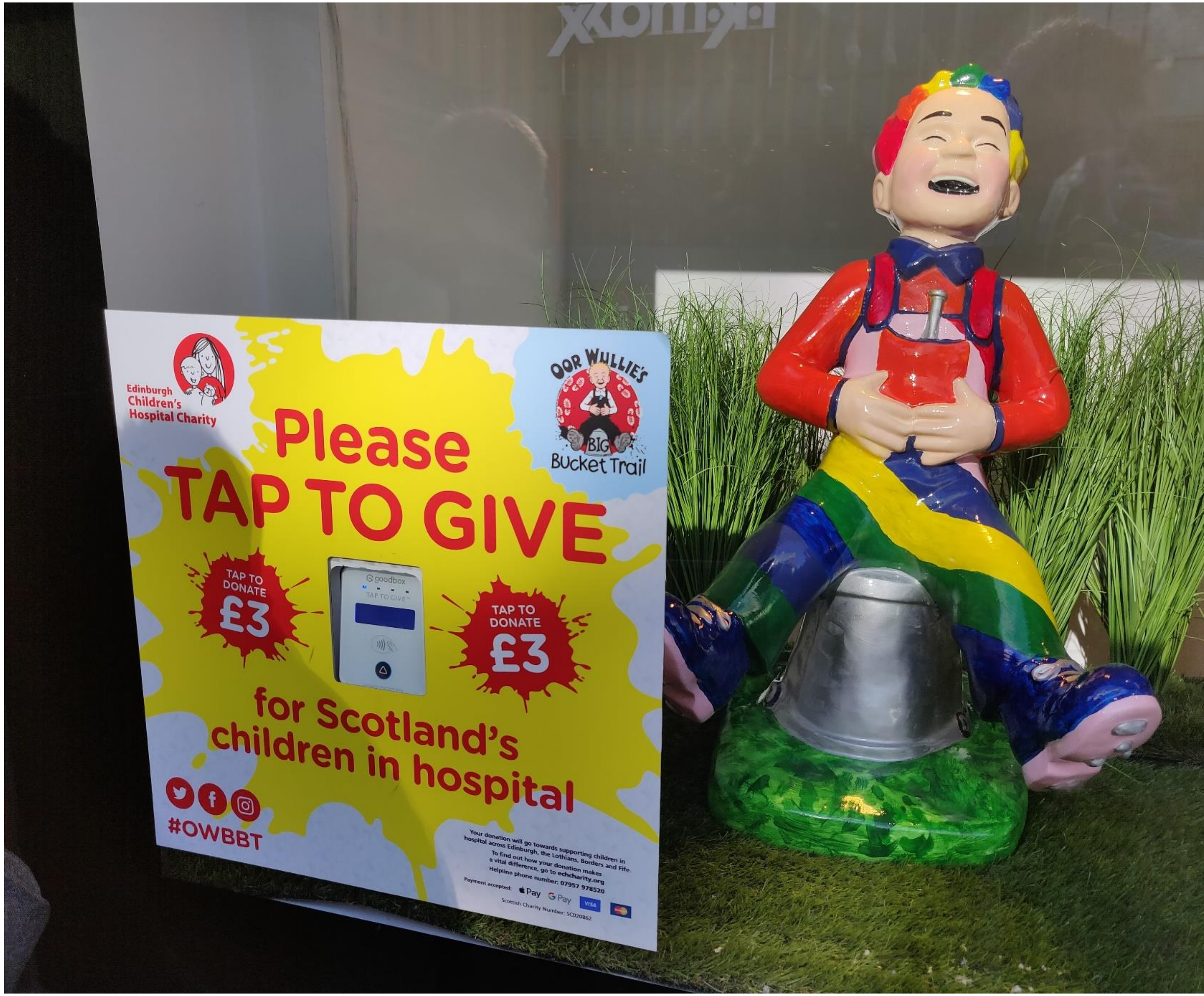
Is this system secure?

- Confidentiality
  - Device might collect data from card like name and card number.
  - Possibly auto-sign people up for marketing.
- Integrity
  - How will you be sure that amount charged really is $10?
- Availability
  - Minimal availability issues because the machine does not take the card away.
  - Minor risk of fraud alert.


OUR VOICE
Victims · Outreach · Intervention · Counseling · Education
OUR MISSION
In the pursuit of a community that is free of sexual violence, Our VOICE serves all individuals in Buncombe County affected by sexual assault and abuse, through counseling, advocacy and education.
35 Woodfin Street
Asheville, NC
Business Line: 828-252-0562
24/7 Crisis Line: 828-255-7576
DIP AND LEAVE A
$10 DONATION
Dip your credit card here to leave a donation!
Insert, remove, and wait for the confirmation.
NORTH CAROLINA GLASS CENTER
Thank you!

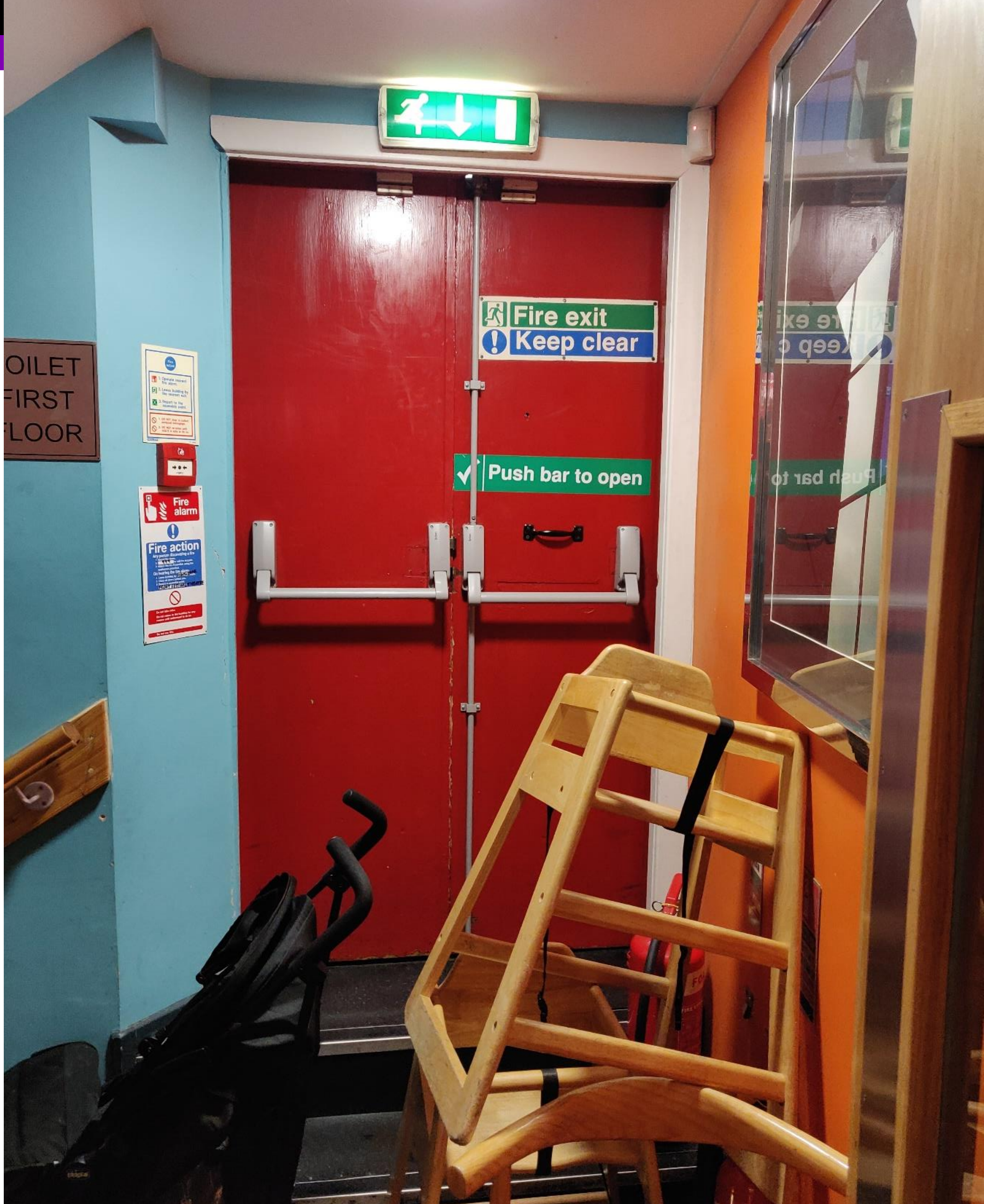
Is this system secure?

- Confidentiality
  - Device might collect data from card like name and card number.
  - Possibly auto-sign people up for marketing. (Unlikely with GDPR)
- Integrity
  - How will you be sure that amount charged really is £3?
- Availability
  - Minimal availability issues, user never looses control of the card.
  - Minor risk of fraud alert.


Edinburgh Children's Hospital Charity
OOR WULLIE'S BIG Bucket Trail
Please
TAP TO GIVE
TAP TO DONATE £3
goodbox
TAP TO GIVE
TAP TO DONATE £3
for Scotland's children in hospital
#OWBBT
Your donation will go towards supporting children in hospital across Edinburgh, the Lothians, Borders and Fife.
To find out how your donation makes a vital difference, go to echcharity.org
Helpline phone number: 07957 978520
Payment accepted: Pay G Pay VISA
Scottish Charity Number: SC020862

Is this system secure?

- Confidentiality
  - Probably fine
- Integrity
  - Maybe
- Availability
  - Big problem



Defining privacy

- The Cambridge Dictionary

- Someone's right to keep their personal matters and relationships secret
  - Controlling personal information
  - *The new law is designed to protect people's privacy*

- The state of being alone
  - Controlling access to self
  - *I hate sharing a bedroom – I never get any privacy*

Controlling who has personal information

Flicker @ElizaC3

Controlling access to self

Think-pair-share

- **Think** about the question to yourself quietly. No talking.
    - 1 minute
- **Pair** with someone sitting near you. Discuss the question and your answers. Lots of everyone talking.
    - 3 minutes
- **Share** through whole-class discussion. A couple groups share their answers and the instructor comments. A couple people talk.
    - About 5 minutes

"Dad, are you using the smart fork?
I'm not receiving any updates...x"
Phil

Uninvited Guests
https://vimeo.com/128873380

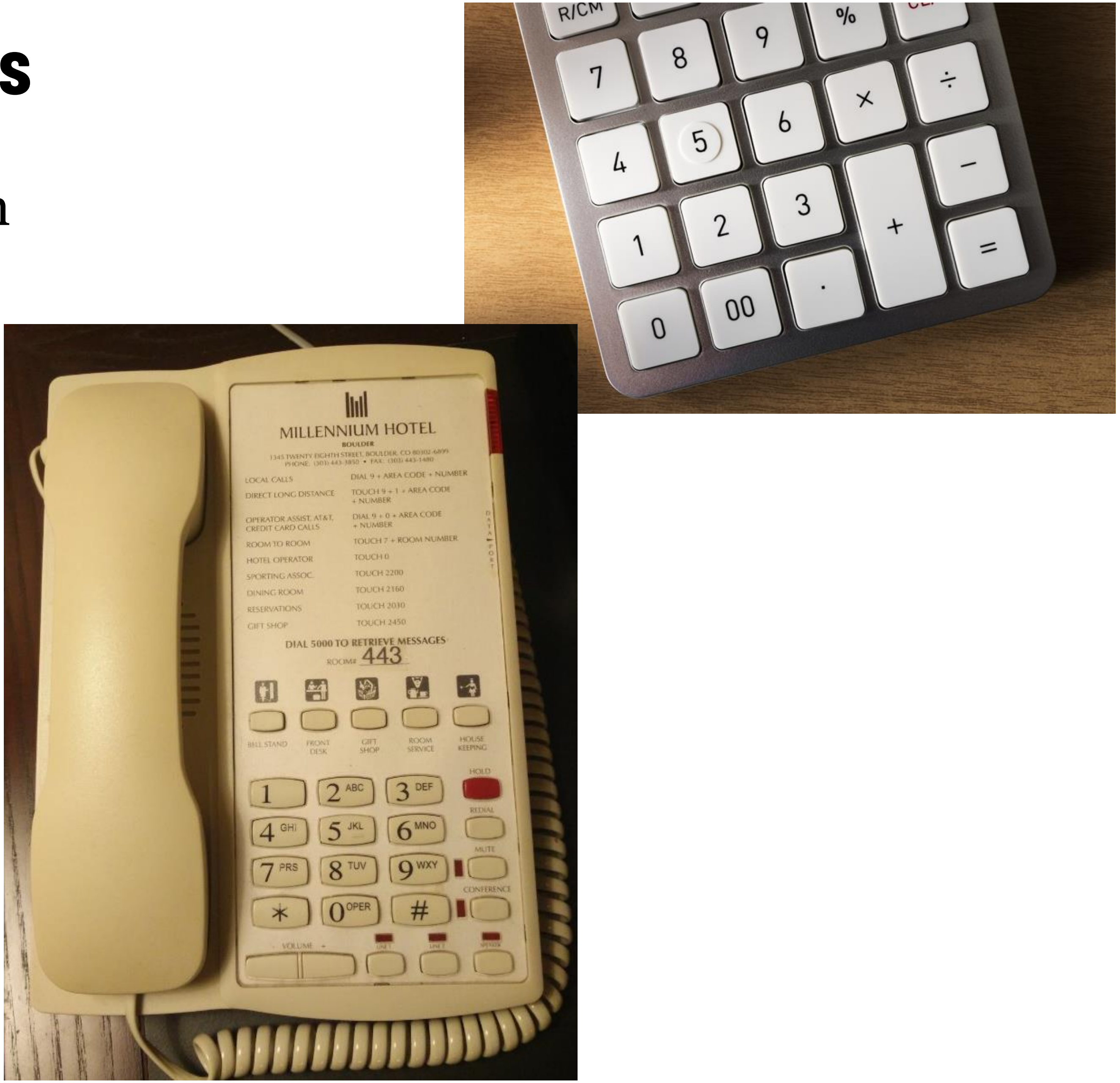
Human-factors Engineering

- **human-factors engineering**, science dealing with the application of information on physical and psychological characteristics to the design of devices and systems for human use.[1]
- Humans are a part of a larger system.
- Human-factors engineers build systems that account for human limitations and support humans in completing tasks with minimal errors.

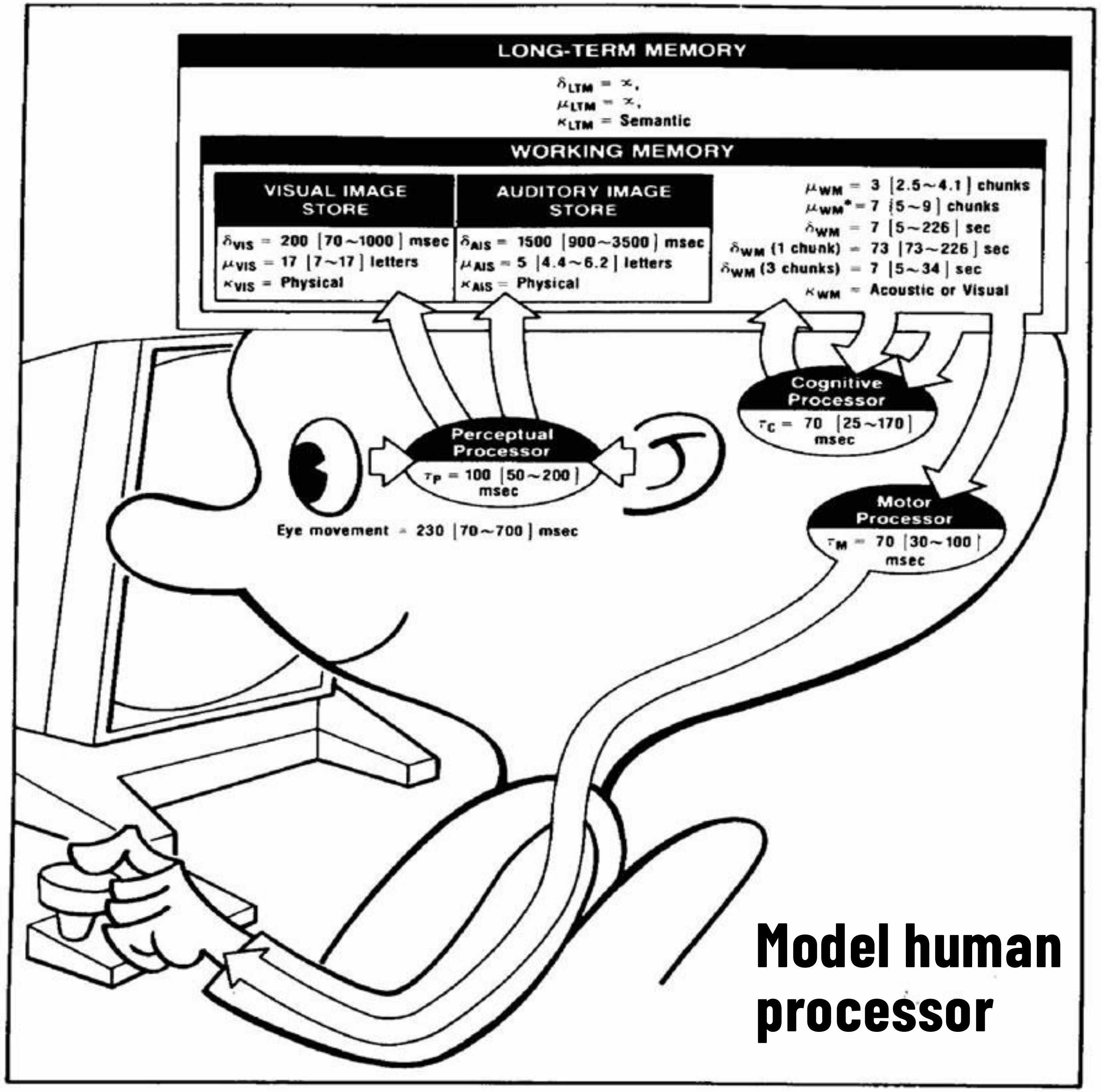
[1] Human-factors engineering, Britanica

Example: calculators vs phones

- Order of the numbers are reversed on phone and calculator
- Extensive testing found that people made fewer dialing errors this way

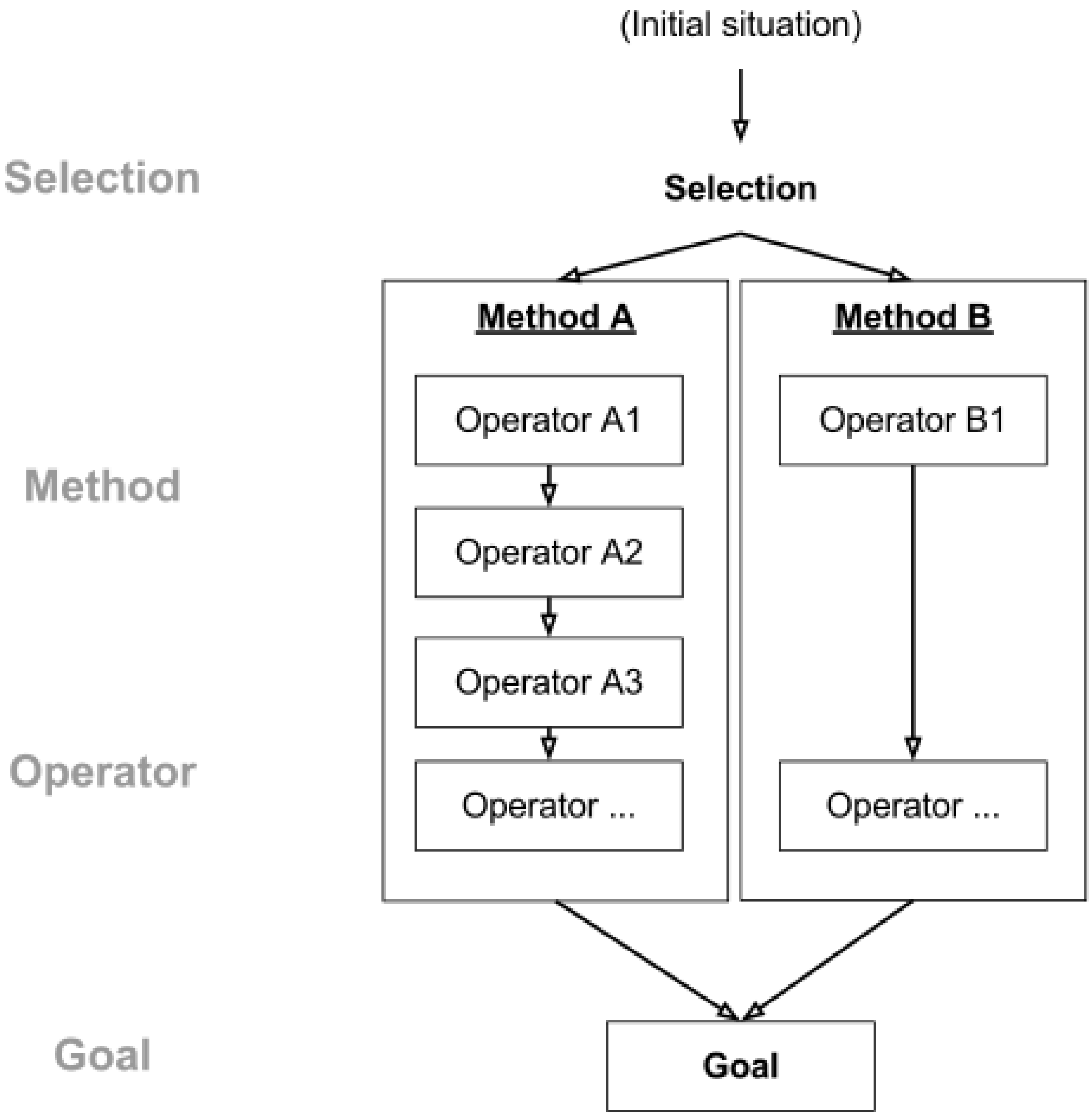

R/CM
%
7 8 9
4 5 6 ×
1 2 3 + ÷ −
0 00 . =
MILLENNIUM HOTEL
BOULDER
1345 TWENTY EIGHTH STREET, BOULDER, CO 80302-6899
PHONE: (303) 443-3850 • FAX: (303) 443-1480
LOCAL CALLS DIAL 9 + AREA CODE + NUMBER
DIRECT LONG DISTANCE TOUCH 9 + 1 + AREA CODE + NUMBER
OPERATOR ASSIST, AT&T, CREDIT CARD CALLS DIAL 9 + 0 + AREA CODE + NUMBER
ROOM TO ROOM TOUCH 7 + ROOM NUMBER
HOTEL OPERATOR TOUCH 0
SPORTING ASSOC. TOUCH 2200
DINING ROOM TOUCH 2160
RESERVATIONS TOUCH 2030
GIFT SHOP TOUCH 2450
DIAL 5000 TO RETRIEVE MESSAGES
ROOM# 443
DATA PORT
BELL STAND
FRONT DESK
GIFT SHOP
ROOM SERVICE
HOUSE KEEPING
HOLD
REDIAL
MUTE
CONFERENCE
1 2 ABC 3 DEF
4 GHI 5 JKL 6 MNO
7 PRS 8 TUV 9 WXY
* 0 OPER #
VOLUME

Some human factors can be computed based on physical characteristics.

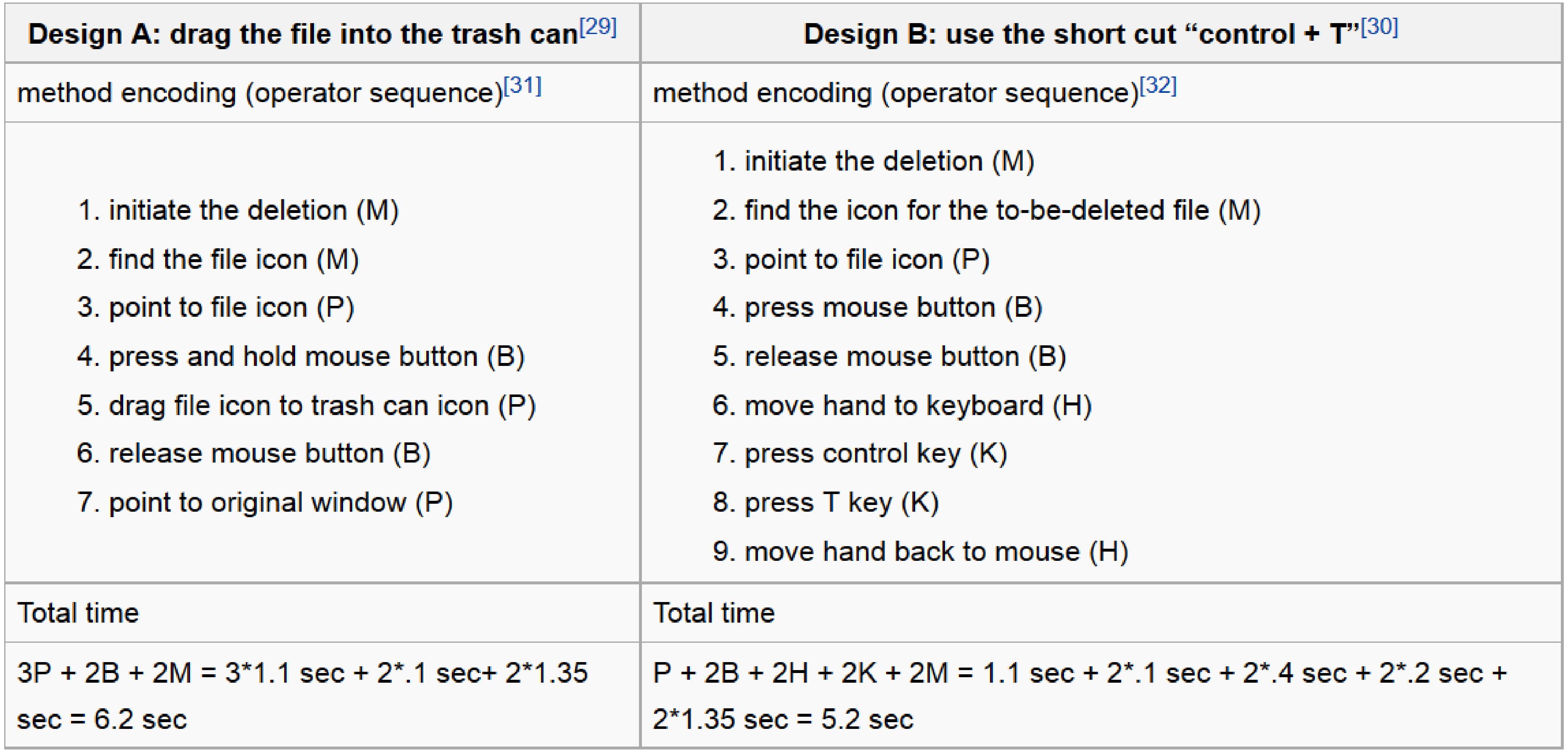

LONG-TERM MEMORY
$\delta_{LTM} = \infty$,
$\mu_{LTM} = \infty$,
κ_{LTM} = Semantic
WORKING MEMORY
VISUAL IMAGE STORE
δ_{VIS} = 200 [70~1000] msec
μ_{VIS} = 17 [7~17] letters
κ_{VIS} = Physical
AUDITORY IMAGE STORE
δ_{AIS} = 1500 [900~3500] msec
μ_{AIS} = 5 [4.4~6.2] letters
κ_{AIS} = Physical
μ_{WM} = 3 [2.5~4.1] chunks
μ_{WM}* = 7 [5~9] chunks
δ_{WM} = 7 [5~226] sec
δ_{WM} (1 chunk) = 73 [73~226] sec
δ_{WM} (3 chunks) = 7 [5~34] sec
κ_{WM} = Acoustic or Visual
Cognitive Processor
τ_C = 70 [25~170] msec
Perceptual Processor
τ_P = 100 [50~200] msec
Eye movement = 230 [70~700] msec
Motor Processor
τ_M = 70 [30~100] msec

Model human processor

Goals, Operations, Methods, and Selection rules (GOMS)



Compare speed of two designs for experts



Design A: drag the file into the trash can[29]	Design B: use the short cut “control + T”[30]
method encoding (operator sequence)[31]	method encoding (operator sequence)[32]
1. initiate the deletion (M) 2. find the file icon (M) 3. point to file icon (P) 4. press and hold mouse button (B) 5. drag file icon to trash can icon (P) 6. release mouse button (B) 7. point to original window (P)	1. initiate the deletion (M) 2. find the icon for the to-be-deleted file (M) 3. point to file icon (P) 4. press mouse button (B) 5. release mouse button (B) 6. move hand to keyboard (H) 7. press control key (K) 8. press T key (K) 9. move hand back to mouse (H)
Total time	Total time
3P + 2B + 2M = 3*1.1 sec + 2*.1 sec+ 2*1.35 sec = 6.2 sec	P + 2B + 2H + 2K + 2M = 1.1 sec + 2*.1 sec + 2*.4 sec + 2*.2 sec + 2*1.35 sec = 5.2 sec

https://en.wikipedia.org/wiki/Keystroke-level_model

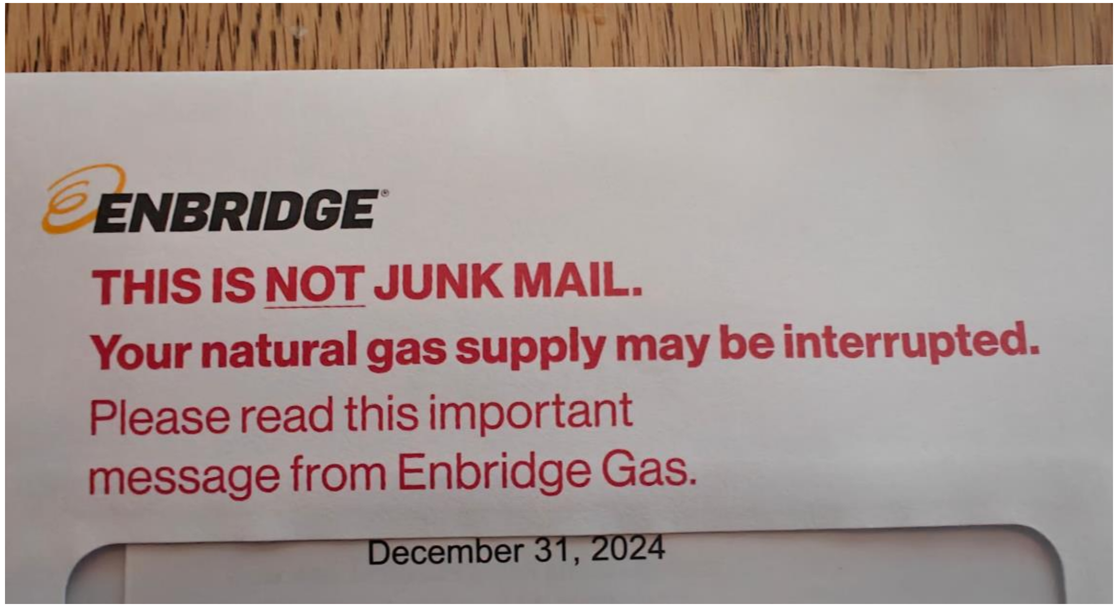
Human Variability

Variability Type	Description	Security Impact
Cognitive	Differences in thinking and information processing	Affects alert comprehension and response time
Behavioral	Varied actions and response patterns	Influences compliance with security protocols
Technical Skill	Different levels of technical experience and knowledge	Determines ability to implement security measures
Emotional	Psychological and stress responses	Impacts decision quality during security incidents

Heavily inspired by Dr Calvin Nobles IMPACT 2025 talk

Error Management Science in Cybersecurity

- **Decision Errors**
  - Poor choices despite having correct information. Often arise from cognitive biases or pressure.
- **Perceptual Errors**
  - Misinterpreting security information. Common with complex dashboards, lots of alerts, or complex interfaces
- **Skill-Based Errors**
  - Failures in execution despite proper intent. Typically occur during routine security tasks.
- **Routine Violations**
  - Deliberately bypassing security protocols. Often due to efficiency-security tradeoffs.


ENBRIDGE

THIS IS NOT JUNK MAIL.

Your natural gas supply may be interrupted.

Please read this important message from Enbridge Gas.

December 31, 2024

Heavily inspired by Dr Calvin Nobles IMPACT 2025 talk

Operationalizing Human Factors Engineering

User Research

Understanding of system users, capabilities, and limitations.

Design Integration

Implementing human-centered solutions into the system's design.

Task Analysis

Identifying critical workflows and decision points.

.

Evaluation

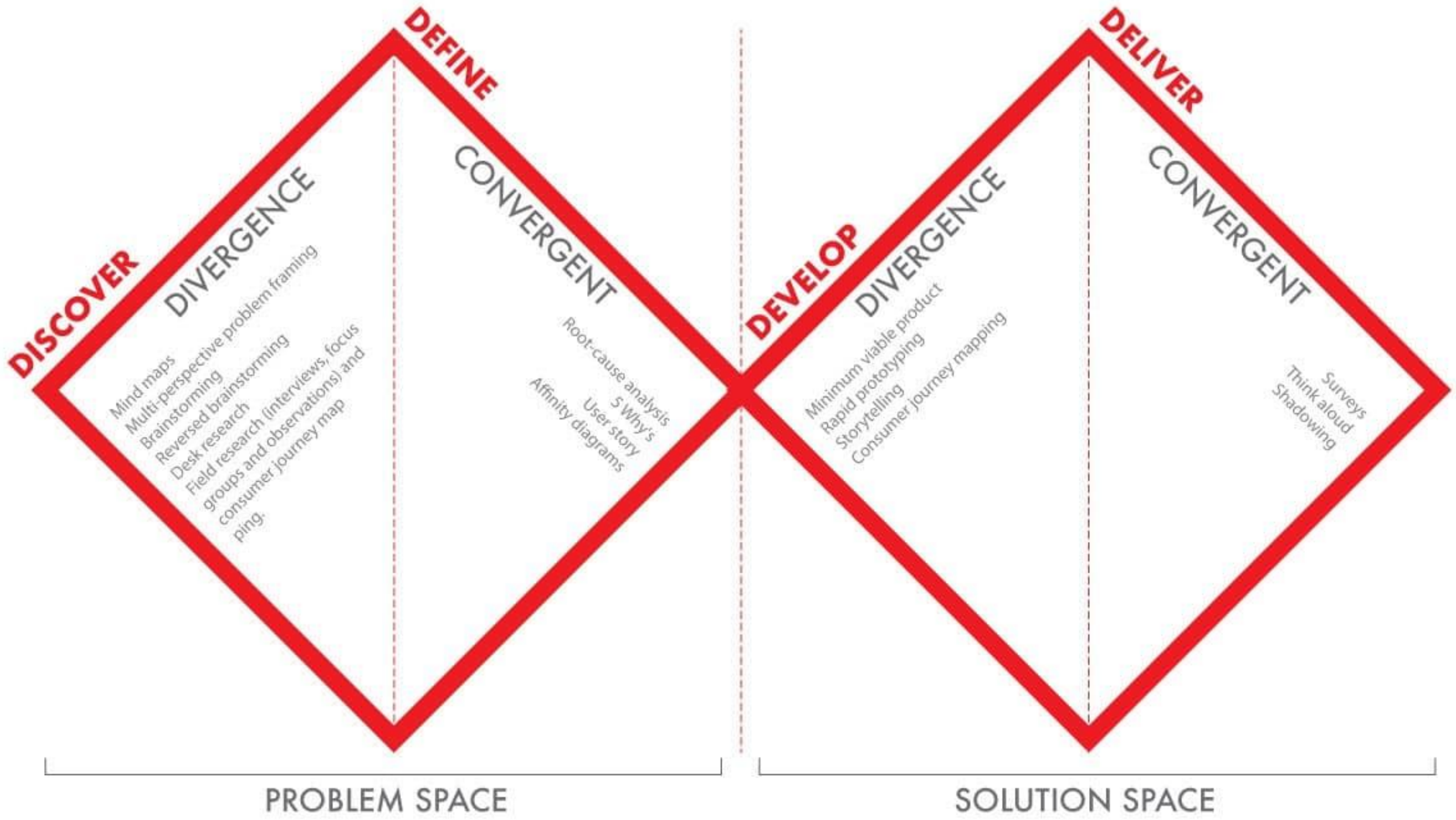
Testing effectiveness against human performance metrics.

Iterative Improvement

Continuous refinement based on human performance data.

Heavily inspired by Dr Calvin Nobles IMPACT 2025 talk

Double Dimond



https://www.gilero.com/resources/understanding-human-centered-design/

Usability (Human-Factors)

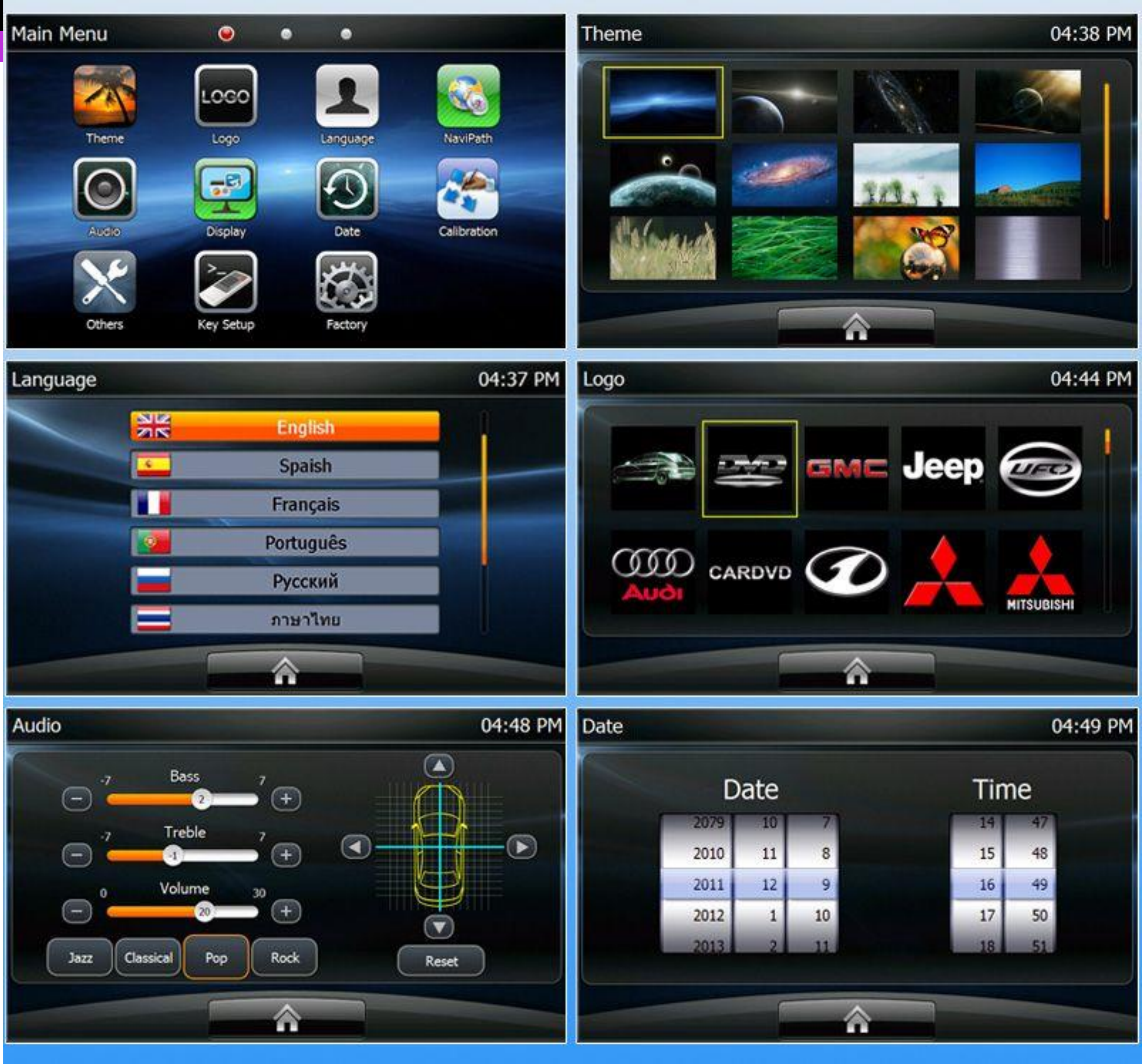
- **Learn-ability** – The type for typical users to learn the actions relevant to a set of tasks.
- **Efficiency** – How long it takes users to perform typical tasks.
- **Errors** – The rate of errors users make when performing tasks.
- **Memorability** – How users can retain their knowledge of the system over time.
- **Subjective Satisfaction** – How users like the various aspects of the system.

Designing the user interface: Strategies for Effective Human-Computer Interaction by Ben Shnelderman

Usability (Human-Factors)

- The rental car navigation system is likely setup for a single user with rare configuration needs – set it and forget it
- Security and privacy issues coming from:
  - Logs
  - Sensors
  - Configuration settings
  - Connection to user’s devices (Bluetooth)

Designing the user interface: Strategies for Effective Human-Computer Interaction by Ben Shnelderman



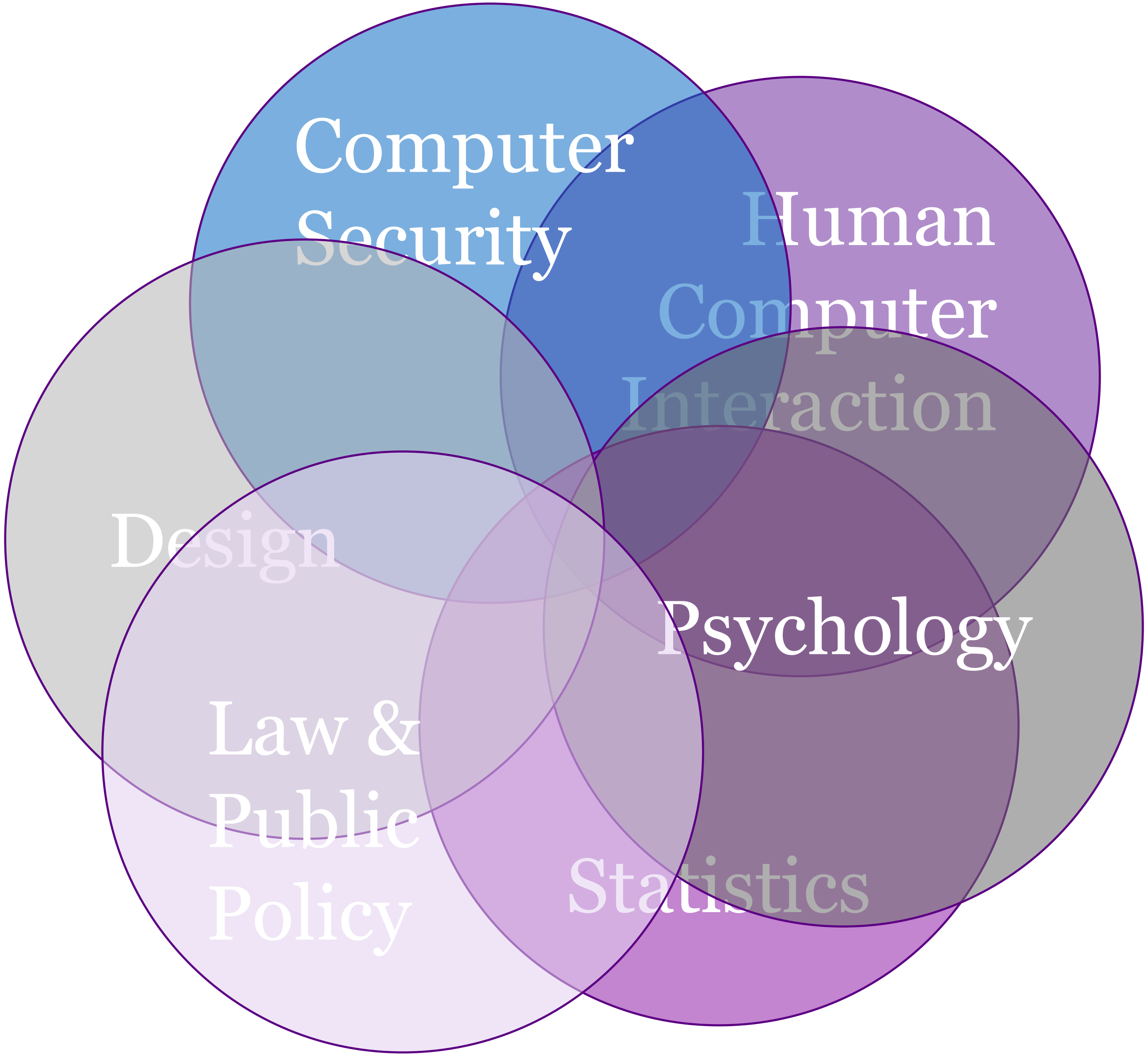
Usability

- **Learn-ability** – Will the user learn that security options exist?
- **Efficiency** – How long do users *think* it will take to perform security tasks?
- **Errors** – Will users notice that security settings need attention? If they do, will they make the correct changes?
- **Memorability** – Does this system use similar configuration such that users can transfer knowledge?
- **Subjective Satisfaction** – Do users feel like they successfully protected themselves?

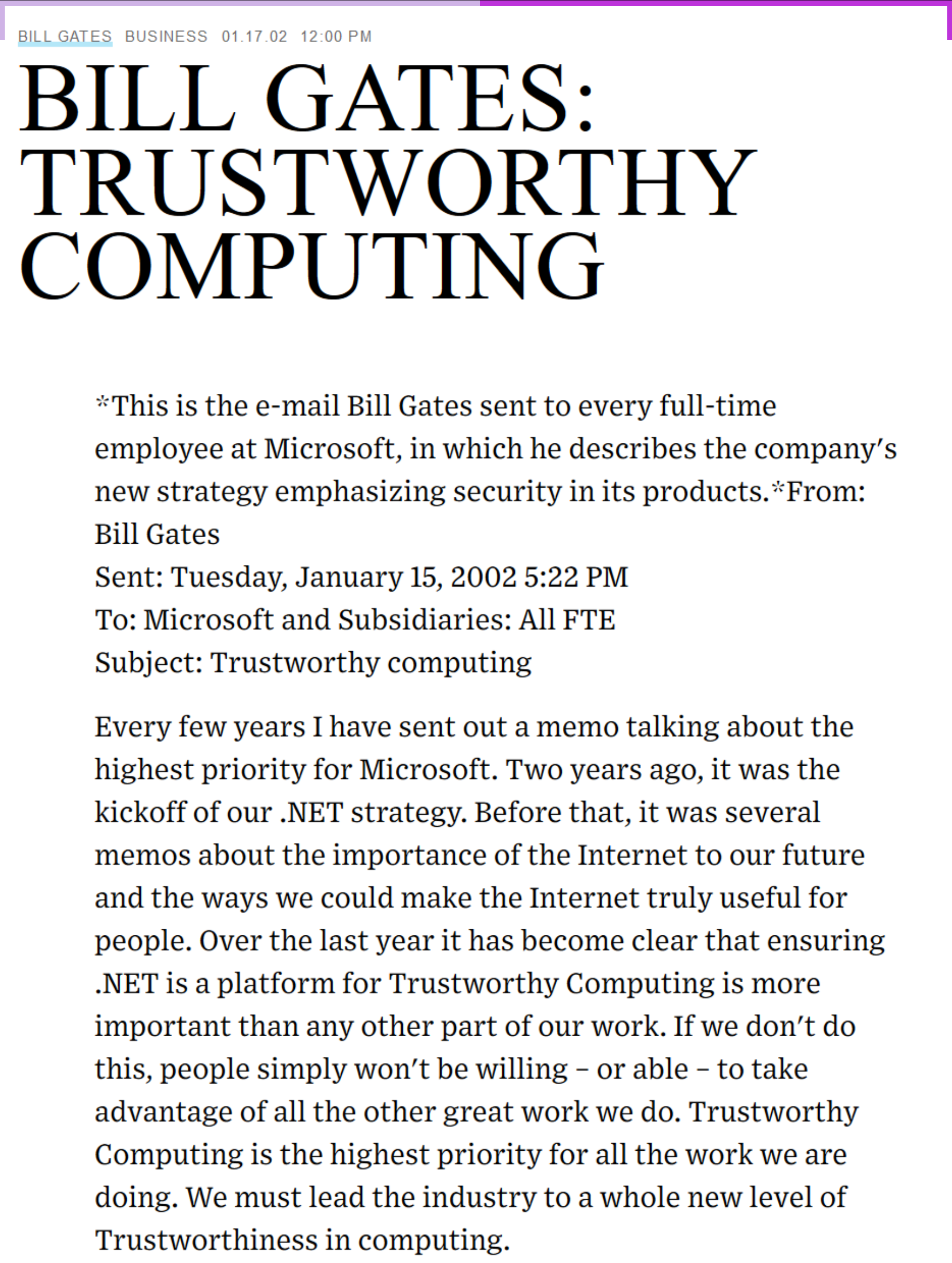
Designing the user interface: Strategies for Effective Human-Computer Interaction by Ben Shnelderman

USec is where security and the real world meet.

It is VERY interdisciplinary



WHAT IS SO CHALLENGING ABOUT USEC?



BILL GATES BUSINESS 01.17.02 12:00 PM

BILL GATES: TRUSTWORTHY COMPUTING

*This is the e-mail Bill Gates sent to every full-time employee at Microsoft, in which he describes the company's new strategy emphasizing security in its products.*From: Bill Gates
Sent: Tuesday, January 15, 2002 5:22 PM
To: Microsoft and Subsidiaries: All FTE
Subject: Trustworthy computing

Every few years I have sent out a memo talking about the highest priority for Microsoft. Two years ago, it was the kickoff of our .NET strategy. Before that, it was several memos about the importance of the Internet to our future and the ways we could make the Internet truly useful for people. Over the last year it has become clear that ensuring .NET is a platform for Trustworthy Computing is more important than any other part of our work. If we don't do this, people simply won't be willing – or able – to take advantage of all the other great work we do. Trustworthy Computing is the highest priority for all the work we are doing. We must lead the industry to a whole new level of Trustworthiness in computing.

Security: The data our software and services store on behalf of our customers should be protected from harm and used or modified only in appropriate ways. Security models should be easy for developers to understand and build into their applications.

Privacy: Users should be in control of how their data is used. Policies for information use should be clear to the user. Users should be in control of when and if they receive information to make best use of their time. It should be easy for users to specify appropriate use of their information including controlling the use of email they send.

Trustworthiness is a much broader concept than security, and winning our customers' trust involves more than just fixing bugs and achieving "five-nines" availability. It's a fundamental challenge that spans the entire computing ecosystem, from individual chips all the way to global Internet services. It's about smart software, services and industry-wide cooperation.

“In the rush to build Internet businesses, many executives concentrate all their attention on attracting customers rather than retaining them. That’s a mistake. The unique economics of e-business make customer loyalty more important than ever.”

E-Loyalty

Your Secret Weapon on the Web

In the rush to build Internet businesses, many executives concentrate all their attention on attracting customers rather than retaining them. That’s a mistake. The unique economics of e-business make customer loyalty more important than ever.

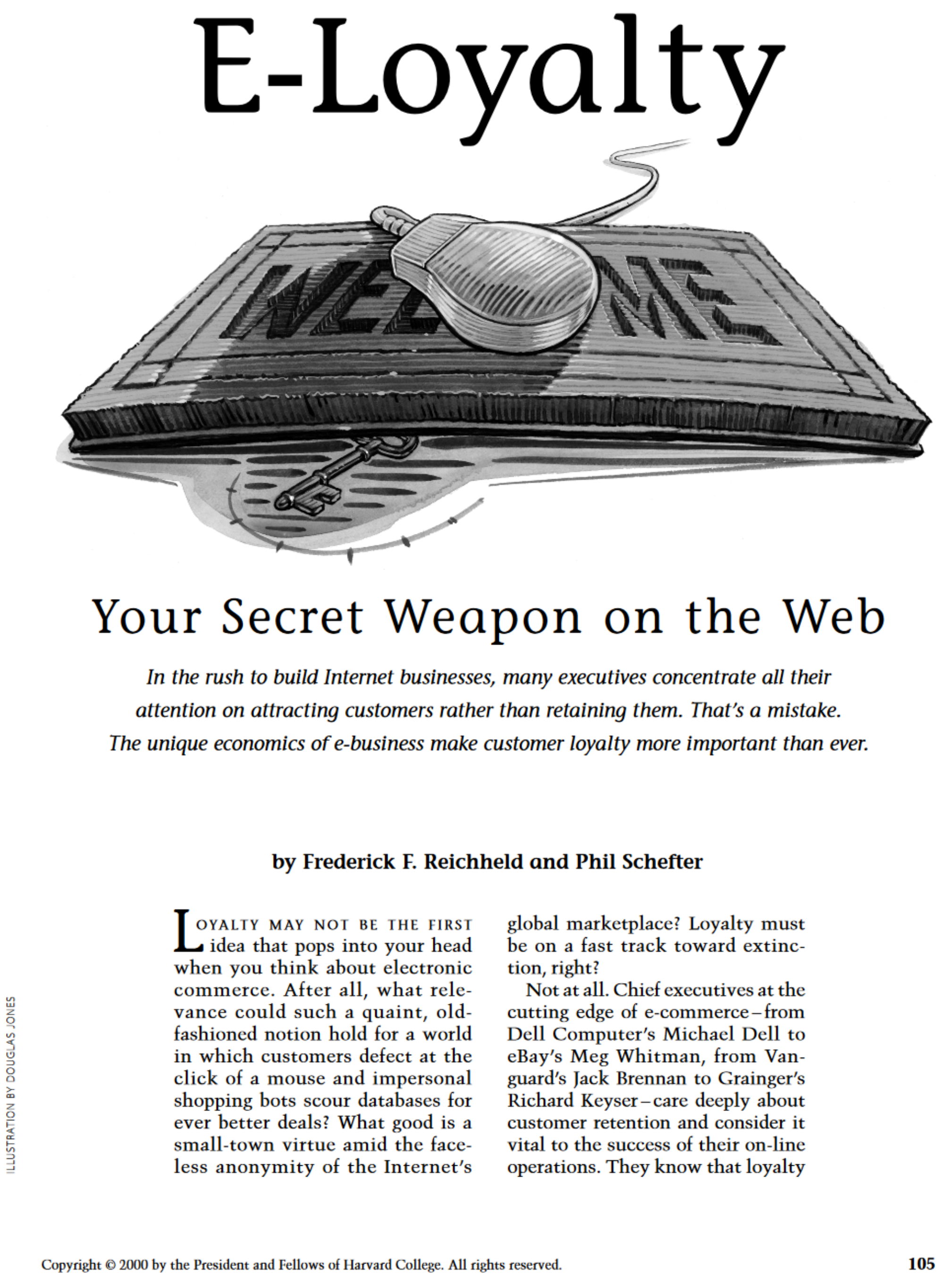
by Frederick F. Reichheld and Phil Schefter

ILLUSTRATION BY DOUGLAS JONES

LOYALTY MAY NOT BE THE FIRST idea that pops into your head when you think about electronic commerce. After all, what relevance could such a quaint, old-fashioned notion hold for a world in which customers defect at the click of a mouse and impersonal shopping bots scour databases for ever better deals? What good is a small-town virtue amid the faceless anonymity of the Internet’s global marketplace? Loyalty must be on a fast track toward extinction, right?

Not at all. Chief executives at the cutting edge of e-commerce–from Dell Computer’s Michael Dell to eBay’s Meg Whitman, from Vanguard’s Jack Brennan to Grainger’s Richard Keyser–care deeply about customer retention and consider it vital to the success of their on-line operations. They know that loyalty

"On the Web … business is conducted at a distance and risks and uncertainties are magnified… Customers can't look a salesclerk in the eye, can't size up the physical space of a store or office, and can't see and touch products. They have to rely on images and promises, and if they don't trust the company presenting those images and promises, they'll shop elsewhere."



E-Loyalty

Your Secret Weapon on the Web

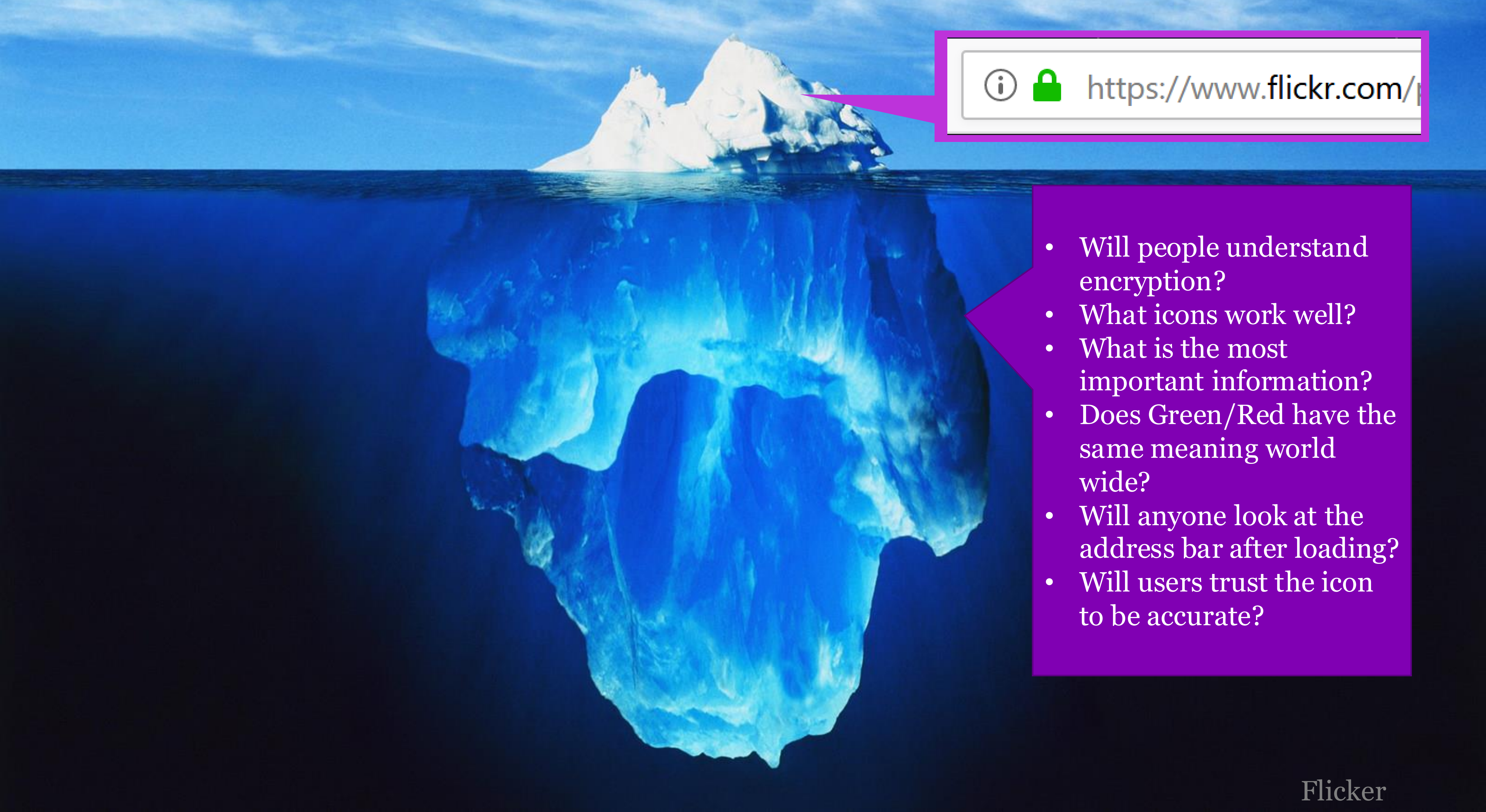
In the rush to build Internet businesses, many executives concentrate all their attention on attracting customers rather than retaining them. That's a mistake. The unique economics of e-business make customer loyalty more important than ever.

by Frederick F. Reichheld and Phil Schefter

ILLUSTRATION BY DOUGLAS JONES

Loyalty may not be the first idea that pops into your head when you think about electronic commerce. After all, what relevance could such a quaint, old-fashioned notion hold for a world in which customers defect at the click of a mouse and impersonal shopping bots scour databases for ever better deals? What good is a small-town virtue amid the faceless anonymity of the Internet's global marketplace? Loyalty must be on a fast track toward extinction, right?

Not at all. Chief executives at the cutting edge of e-commerce–from Dell Computer's Michael Dell to eBay's Meg Whitman, from Vanguard's Jack Brennan to Grainger's Richard Keyser–care deeply about customer retention and consider it vital to the success of their on-line operations. They know that loyalty



- Will people understand encryption?
- What icons work well?
- What is the most important information?
- Does Green/Red have the same meaning world wide?
- Will anyone look at the address bar after loading?
- Will users trust the icon to be accurate?

Flicker

Questions