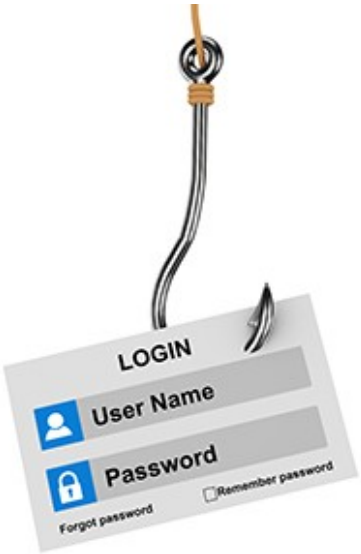
CSE 3400 - Computer and Information Security Topic 8:

Phishing and Usable Security

Last updated: 4/21/20

“Companies spend millions of dollars on firewalls and secure access devices, and its money wasted because none of these measures address the weakest link in the security chain the people who use, administer and operate computer systems”
--Kevin Mitnick, Ghost in the Wires.



Usable security (bad?) example

The Usable Security Challenge

- Goal: design systems to provide security for ‘normal people’
- ~~Challenge: “Users are stupid, negligent, don’t care, and don’t understand risks and technology~~
- Challenges:
  - System designers focus on well-defined goals
  - Secure-usage requires non-natural behavior

When most people don’t use security tools correctly, the problem is with the tools, not with the people.
[Steve Bellovin]

The Usable Security Challenge

- Goal: design systems to provide security for ‘normal people’
  - Against eavesdropping – using encryption:
    Why Johnny can’t Encrypt [WhittenTyger99]
  - Against phishing - using browsers:
    Why Johnny can’t Surf (safely) [H09]

- Challenges:
  - System designers focus on well-defined goals
  - Secure-usage requires non-natural behavior

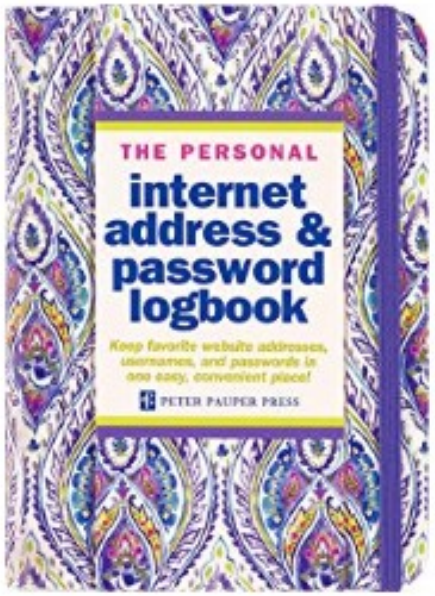
When most people don’t use security tools correctly, the problem is with the tools, not with the people.
[Steve Bellovin]

User Authentication

- Something you know
  - Passwords, pattern, Q&A, recognition
- Something you have
  - A device, e.g., smartcard, containing private key
  - A device with secure connection, e.g., phone
  - Cookies stored in browser
- Something you are – biometrics
  - Fingerprint, voice, face, iris, hand,…
  - Static, dynamic or continuous (e.g., gait)
- Somebody you know: known friends

Passwords…

- The classic `something you know' defense
- Many problems…
  - Weak: ~50% of PWs are in `dictionary' of 1M PWs
    - Dictionary, offline attack + user-specific guessing
  - Password reuse
    - Too many sites
    - Forcing users to change PWs…
  - Users' lists of passwords
  - Exposure of PW databases
  - And… phishing attacks
    - Users disclosing pws to rogue site

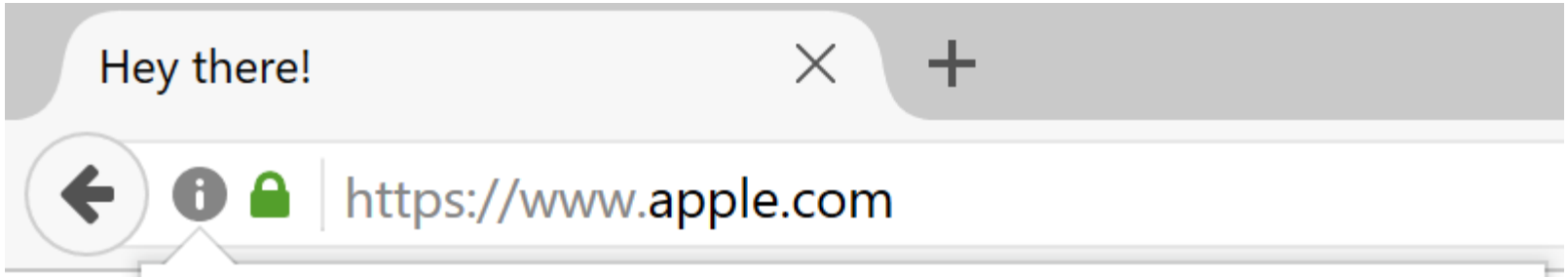


Rogue Website Attacks

- Attack types
  - Scams and malware-download
  - Exploit browser and/or site vulnerability
  - Use browser resources for DoS on sites
  - Phishing: Disguise as trusted site, steal PW etc.
    - Spear-phishing: same but tailored to specific user
    - Homographic: misleadingly-similar domain
      - Similar letters, Unicode letters
    - Typos-attack: misspelling of domain name
- Phishing is still the main tool for cybercrime
  - Easy, simple and very effective

Homograph/Punicode Attacks

- Homograph phishing: use of visually-similar characters, e.g. B0A vs. BOA
- Punycode: ASCII encoding of Unicode characters, to allow non-Latin domain names
- Non-Latin letters may `clone' Latin chars

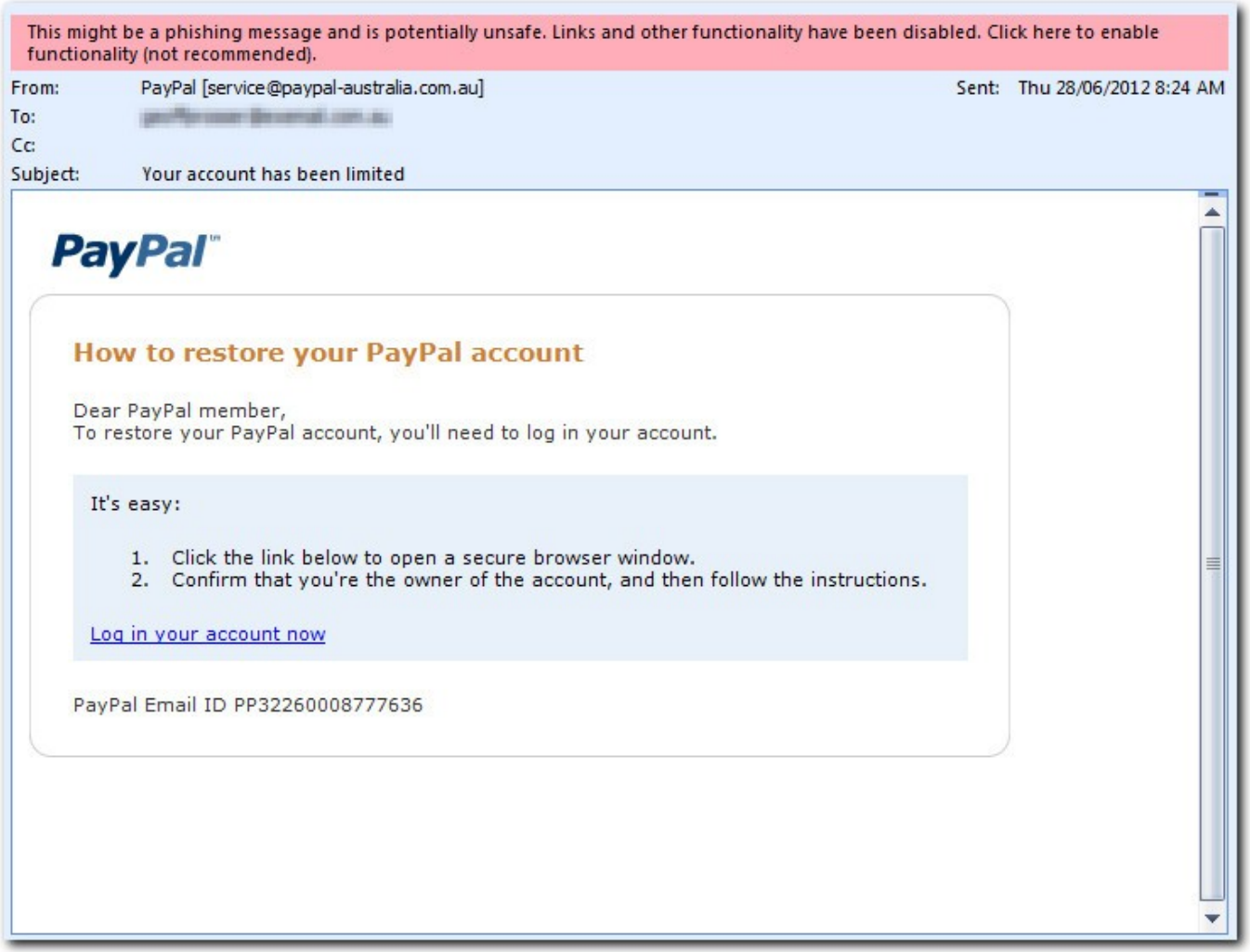


  - Cyrillic "a" (U+0430), not ASCII "a" (U+0061)
  - Defense: `forbid' mixed fonts (may fail – all Cyrllic)

How users reach rogue/phishing sites?

- MitM attack (unprotected search engine)
- (‘Blackhat’) Search Engine Optimization
- Ads, malware, ……
- Take-over (‘deface’) legit-site
- Phishing links (in email, social-net,…)
- Users should not follow these links!!
  - Can’t we teach users not to follow them??
  - Typical `user education’
- Mis-typing

Phishing Email – Example



This might be a phishing message and is potentially unsafe. Links and other functionality have been disabled. Click here to enable functionality (not recommended).

From: PayPal [service@paypal-australia.com.au] Sent: Thu 28/06/2012 8:24 AM
To:
Cc:
Subject: Your account has been limited

PayPal™

How to restore your PayPal account

Dear PayPal member,
To restore your PayPal account, you'll need to log in your account.

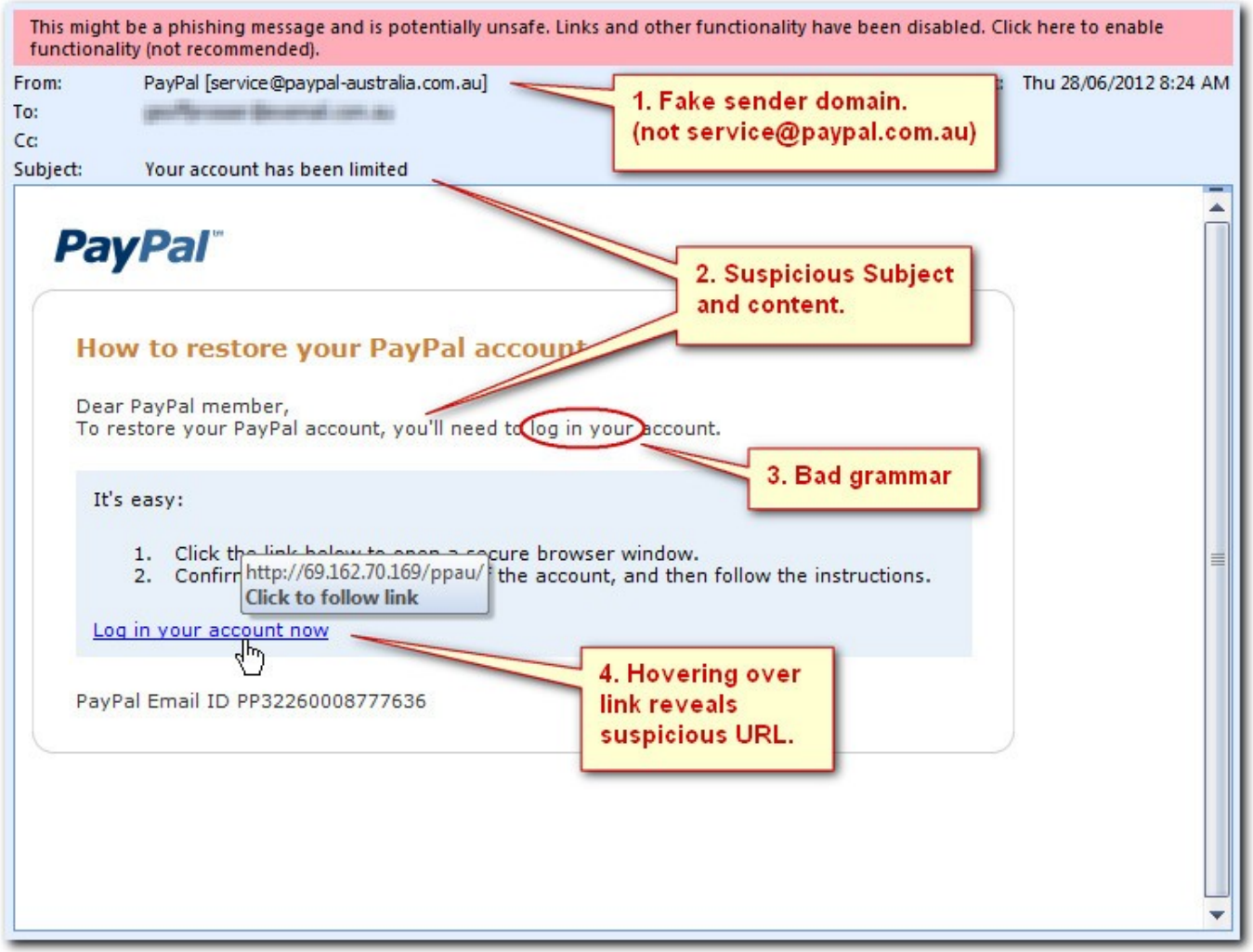
It's easy:

1. Click the link below to open a secure browser window.
2. Confirm that you're the owner of the account, and then follow the instructions.

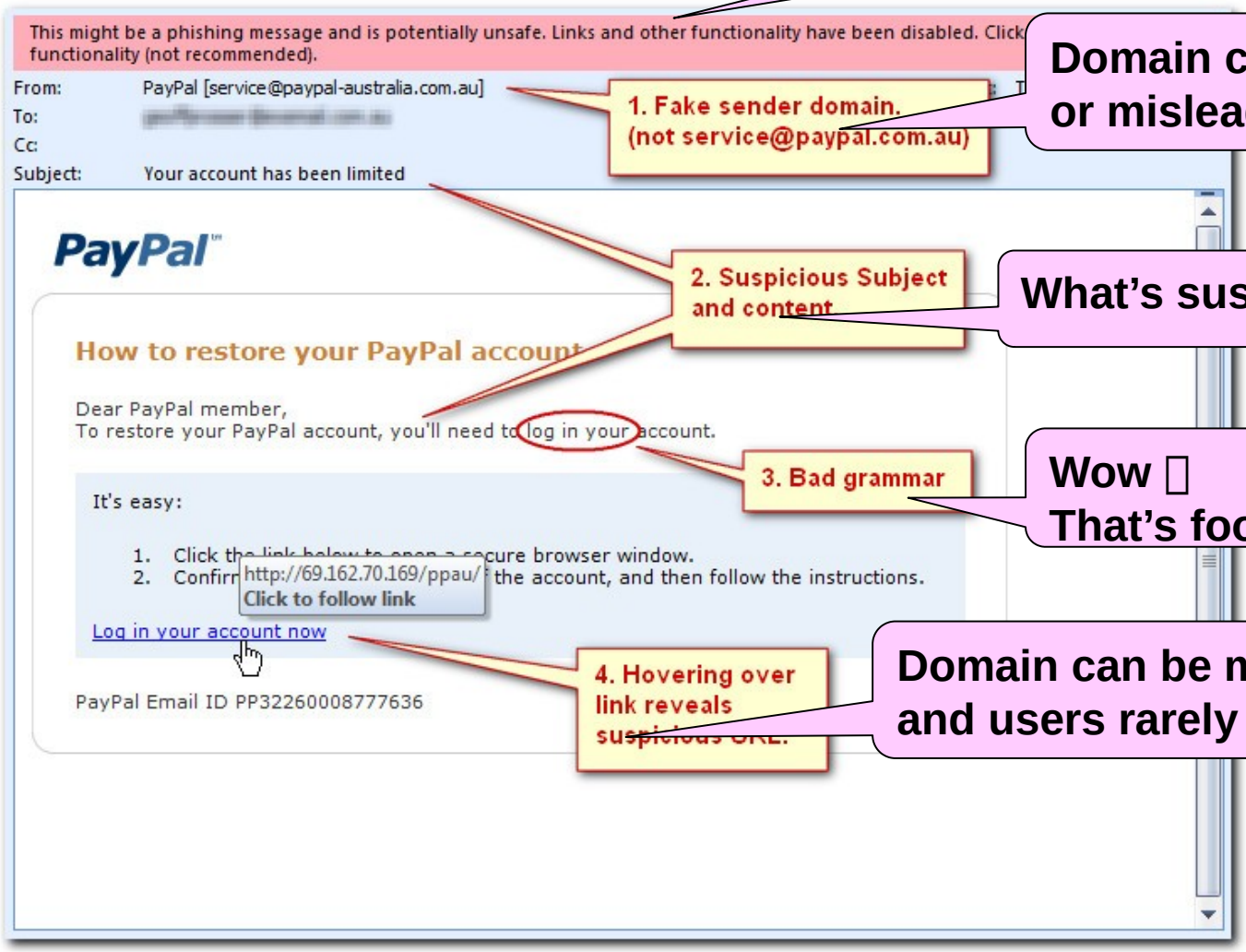
Log in your account now

PayPal Email ID PP32260008777636

Phishing Email: Signs (1)



Phishing Email: ‘Signs’ (2)



Unreliable detection

Domain can be fake or misleading

What’s suspect?

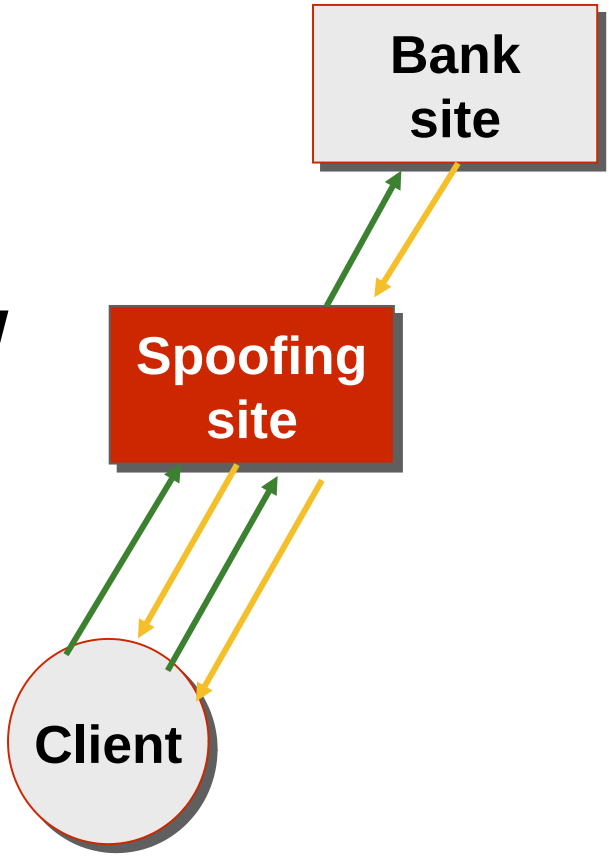
Wow □
That’s fool-prove□

Domain can be misleading, and users rarely `hover’

Web Spoofing Attack

- **Can't user detect spoofed site?**
- **Web spoofing attack:**
  - **Copy & modify target website**
  - **User visits the spoofing site**
  - **User exposes personal info, e.g., PW**

- User is not aware
  - Spoofing site can forward information to the target, to avoid detection
  - Detect incorrect location (URL)?
  - Most users do not notice
  - Or – spoof the location bar too…



Existing Site/Security Indicators

- Browser Passive Indicators
  - Address bar, http/https prefix, padlock

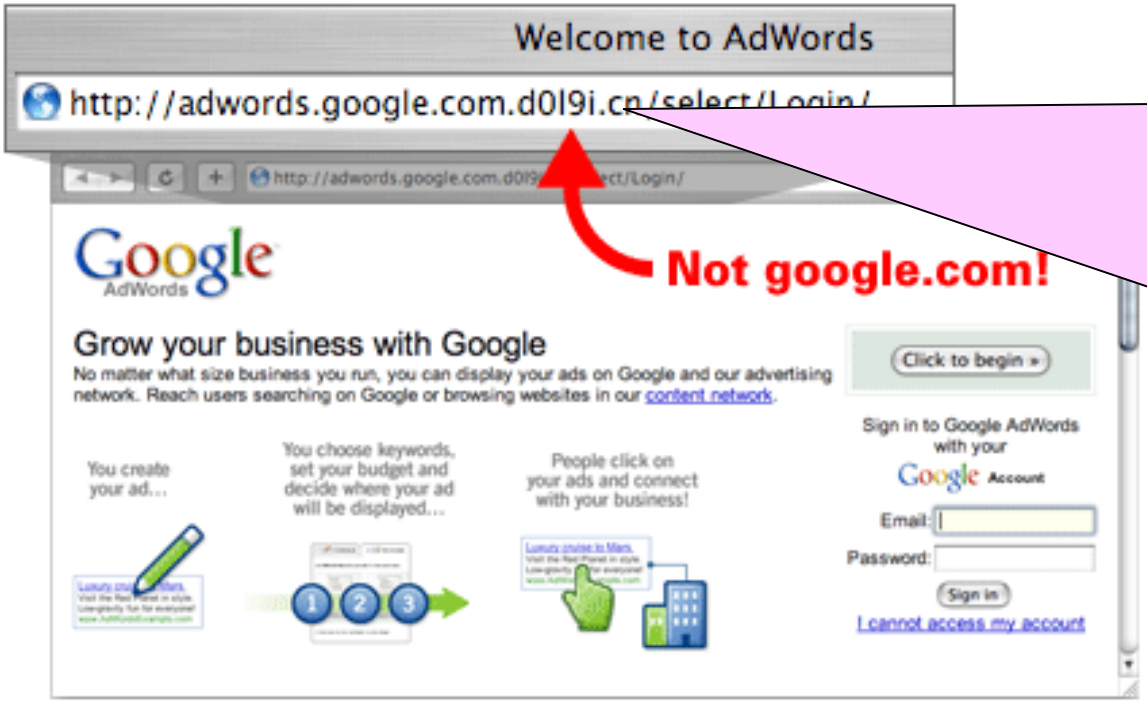
Secure | https://www.google.co.il

https://www.google.co.il/?gws_rd=ssl

https://www.google.co.il/?gws_rd=ssl#spf=1

Users may not understand or pay attention to these passive indicators (Schechter et al., 2007; Karlof et al., 2009 and more)

Browser Identity/Security Indicators



Location Bar:

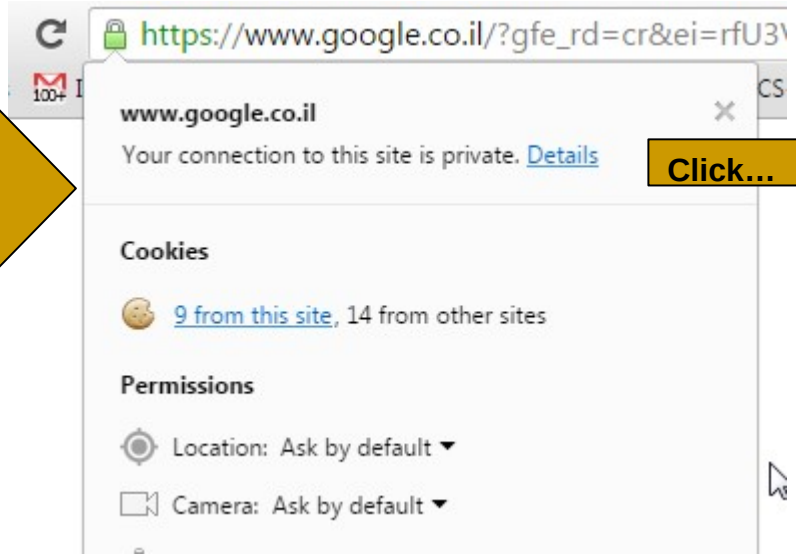
- **Domain name**
- **TLD at <u>right</u> hand**
- **Separated by dots**
- **Followed by path**
- **Hard to detect!**

Visibility and Focus (Violated) usability principle:
Make critical info stand-out, easily distinguished from other info – esp. from site-controlled info!

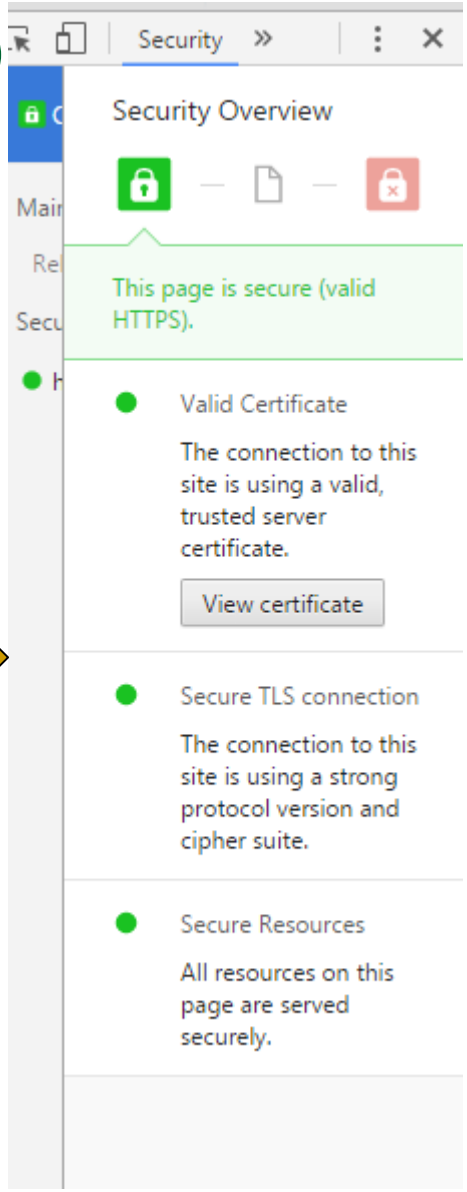
Browser Trust Indicators

Browser Trust Indicato

Click on padlock



Click…



Few usable-security principles…

- Users focus on their goals, not on security
  - Users <u>don't</u> click on padlock etc.
- 'Click-whirr syndrome': automated, mindless response to repeating situation
  - See login page? Enter pw and click login!
  - Same warning? Ignore!
- Cryptography is in Greek
  - Security UI: intuitive – or to shrink responsibility?
  - URLs, Domain-Names are also `in Greek'
  - x.y.z vs. z.y.x vs. vs. v.w/x.y.z vs. x-y.z vs…

Defenses against Phishing Websites

- Trust Indicators
  - Research shows: limited impact
- HSTS: site _always_ uses TLS (https)
- Avoid/reduce dependency on passwords
  - Cookies, 2nd factor authentication (2FA)
  - What of TLS/SSL client authentication ?
- Preventing phishing-sites:
  - Don’t register, certify too-similar domain names
  - CT: detect certs to same/similar DN
  - **Blacklist** suspect sites (browser/search-engine)

Security of Anti-Phishing Blacklists

- Anti-phishing blacklists work <u>if</u>:
  - Browser blocks suspect site
    - And user does not circumvent
    - Or browser warns, and users heeds the warning
  - Phishing domain is in blacklist
    - Fails for new domains
    - Fails for hosted phishing sites (using scripts/applets)
    - Fails for MITM / DNS-poisoning adversaries
- Users, vendors love blacklists
  - Easy trust model: all (unblocked) sites are Ok
  - But IPs and domains are cheap & many sites broken
  - False sense of security

Few more usable-security principles…

- Users expect security-by-default
  - Expect default operations to be secure
  - Don't even ask me if there is a risk
- Users expect infallible defenses
  - Why is it a defense, if it may still fail?
- **Illusion of security worse than no security**
  - Challenge: 'really' protect user – avoid illusions

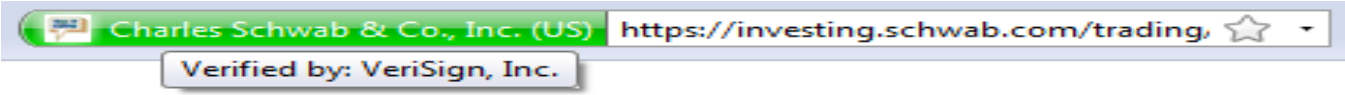
Defenses against Phishing Websites

- Trust Indicators [limited impact]
- HSTS: site _always_ uses TLS (https)
- Reduce dependency on passwords: cookies, 2FA
- Preventing phishing-sites:
  - Don’t register, certify too-similar domain names
  - CT: detect certs to same/similar DN
  - **Blacklist** suspect sites (browser/search-engine)
- **Empower user:**
  - **Better identity and trust indicators/mechanisms**
  - **Educate and train users**

Trust Indicators are **Passive**

- None ('basic' browser indicator only)

- Name of site & CA (from certificate)



- Warning

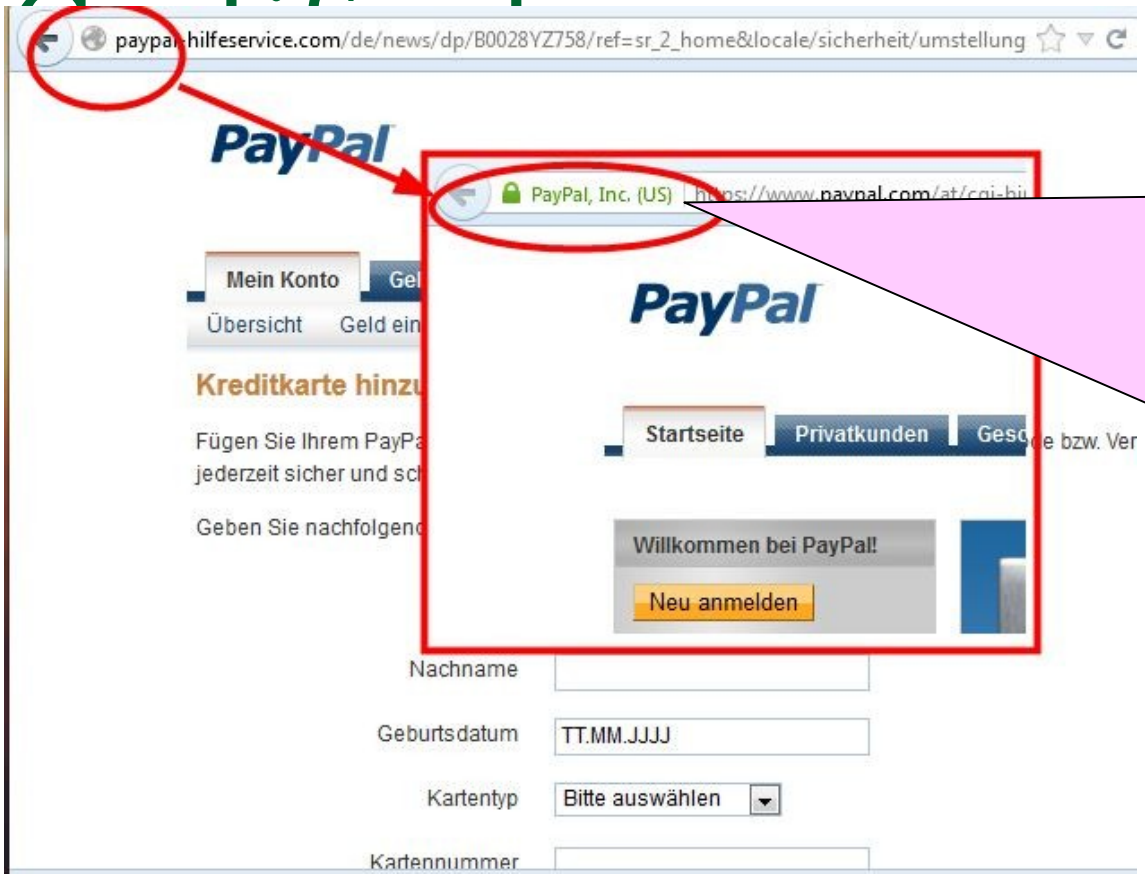
- User-selected text/image for site (e.g. Yahoo!'s sign-in seal)

Cryptography is in Greek – and also domain names? BoA example

Secure (S)? Insecure (I)? Attack (A)? Can't tell (C)?

www.BOA.accts.com		www.accts.BOA.com	
https://www.accounts.BOA.c..		https://www.accts.BOA.com	
https://www.BOA.com.accts		http://www.accts.BOA.com	
https://www.acctsBOA.com		https://wwwaccts.BOA.com	
https://www.BOA.com/accts		https://www.accts.B0A.com	
https://www.BOAcom/accts		https://wwwBOA.com/accts	

Extended-Validation



'Extended Validation (EV)' certificate:

- **'More secure' validation by CA**
- **Indicate <u>name</u>**
- **'Better padlock'**

The Chrome Princ

- What is Chrome?
  - ~~Name of browser~~
  - Jargon: user-interface surrounding web page
  - URL, toolbars, buttons, tabs, scrollbars, status…
- **Principle: users don't know what is chrome**
  - Don't distinguish btw (untrusted) content from site vs. (trusted?) content from browser (in Chrome)
  - Padlock vs. fav-icon or even vs. pix of padlock
- And in mobiles? Often no 'real' Chrome !

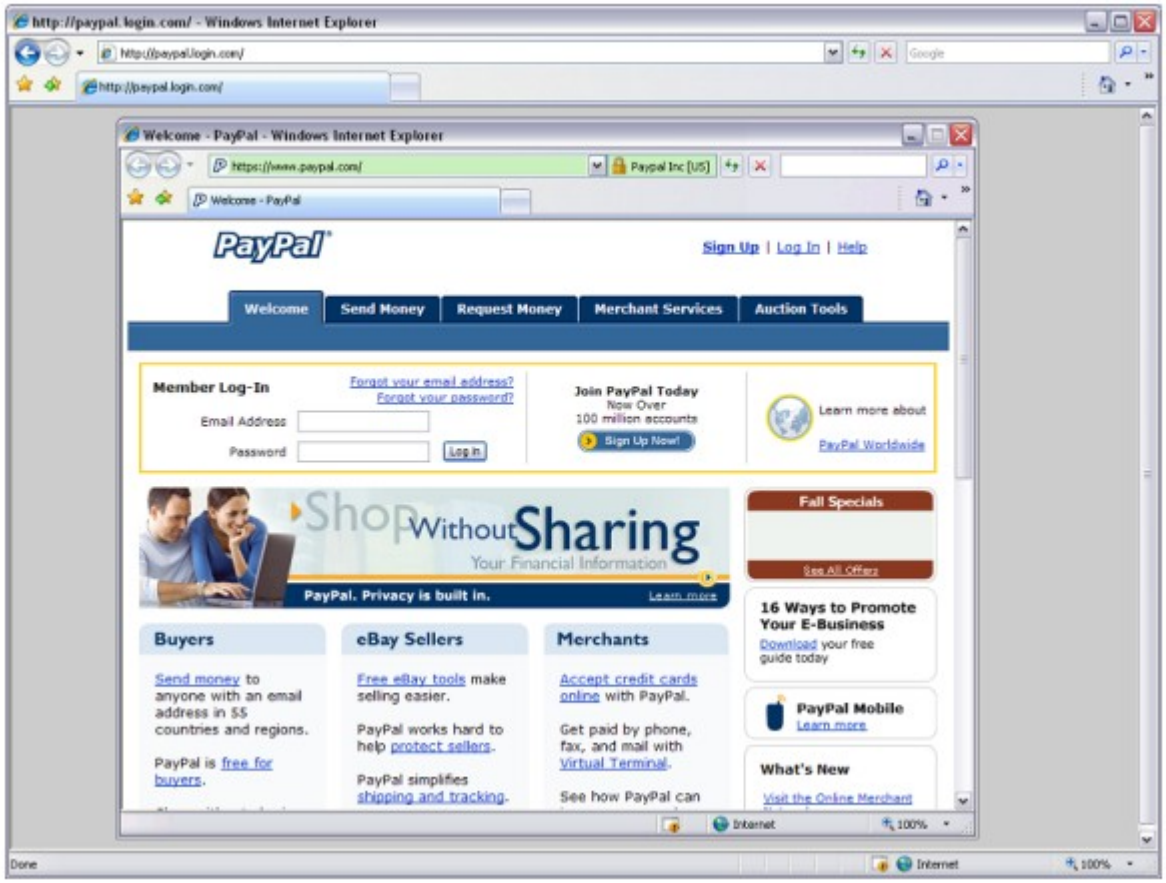
Indicators in Mobile Browsers?

- Trust ‘level’: can you see it?
- Domain: TLDs etc. may be ‘cut’ [from RHS!]
  - Even for legit, reasonable domain names
  - Same in most mobile browsers

- Some websites can also foil any browser…

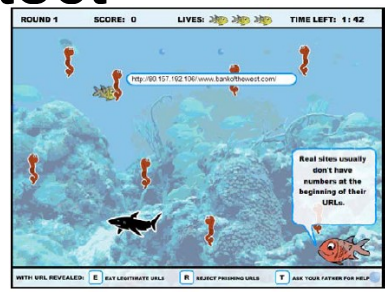
Picture-in-Picture Attack

Even if users understand Chrome, would they notice Fake Chrome?



Secure use via Education and Training

- Train users to detect phishing emails [Kumaraguru09]
- Anti-Phishing Phil game: train users to detect phishing websites using browser passive indicators [Sheng*07]



- Or: continuous test and praise
  - Tests done during normal use of the system
  - Give feedback (praise) to users

Measuring Detection: Challeng

Short-term lab studies

Awareness to study's purpose more cautious than real life

Unaware less cautious than real life

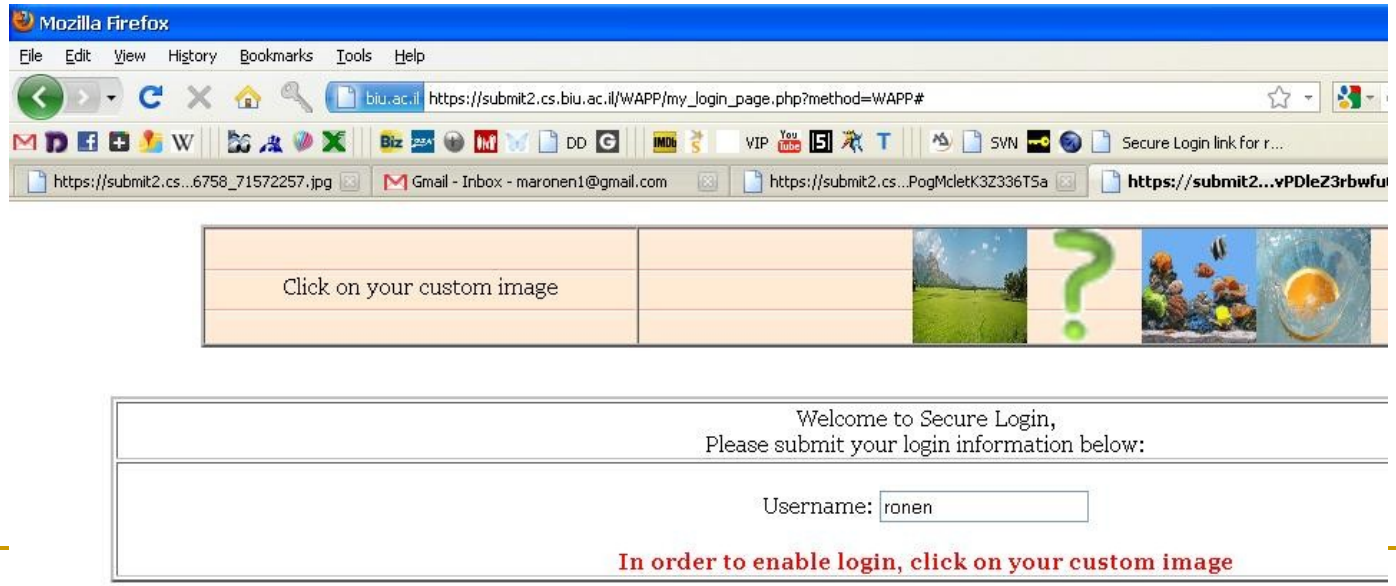
Rather high detection rates, 63-95% [DTH06, WMG06, HJ08]

Low detection rates 3-40% [DTH06, WMG06, SD*07]

Very low detection rates, 0-8% [WMG06, SD*07, HJ08]

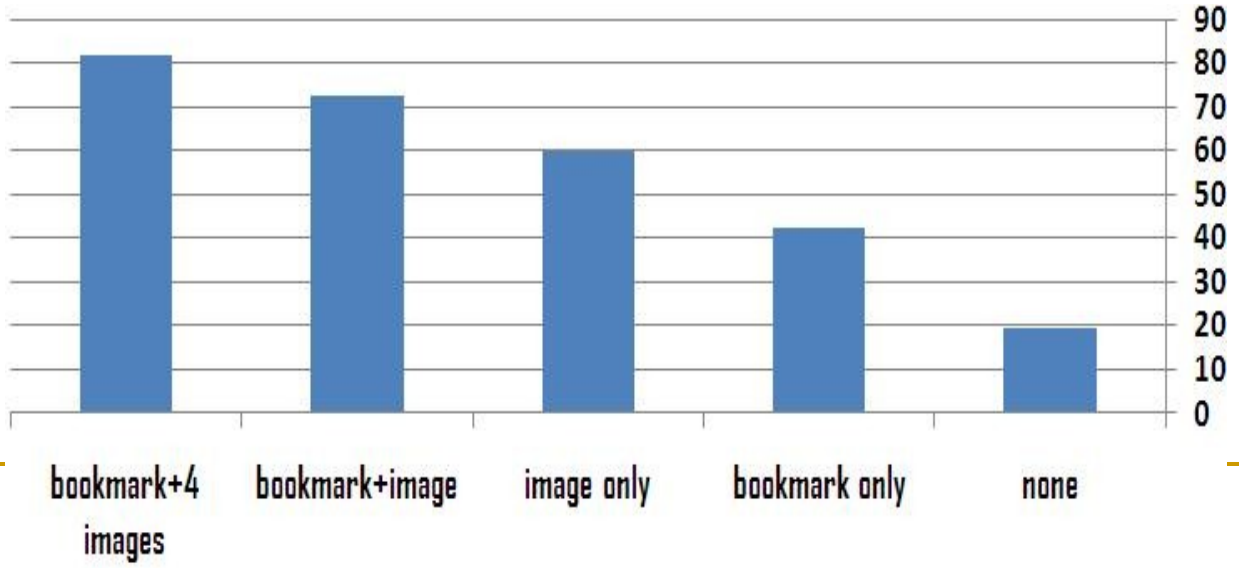
Anti-Phishing: Long-Term Studies

- [H+Jbara04, 08]: improved browser indicators
  - □ significant but insufficient improvement in detection rates: from ~20% to ~40%
  - Indicators (partially) adopted by browsers
- [H+Margulis11]: <u>active</u> (site) indicators



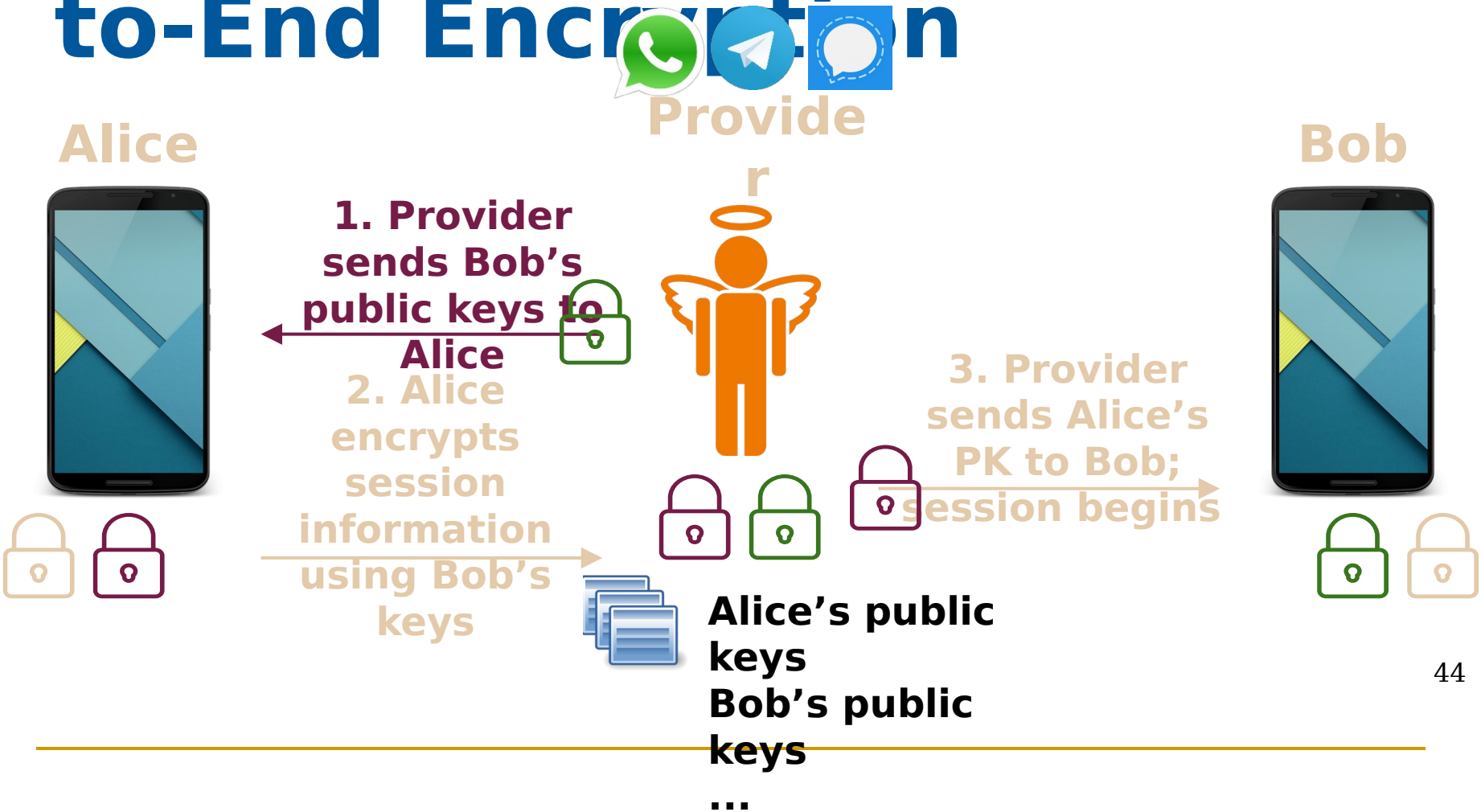
Anti-Phishing: Long-Term Studies

- [H+Jbara04, 08]: improved browser indicators
  - □ significant but insufficient improvement in detection rates: from ~20% to ~40%
  - Indicators (partially) adopted by browsers
- [H+Margulis11]: <u>active</u> (site) indicators
  - Plus: secure bookmark mechanism

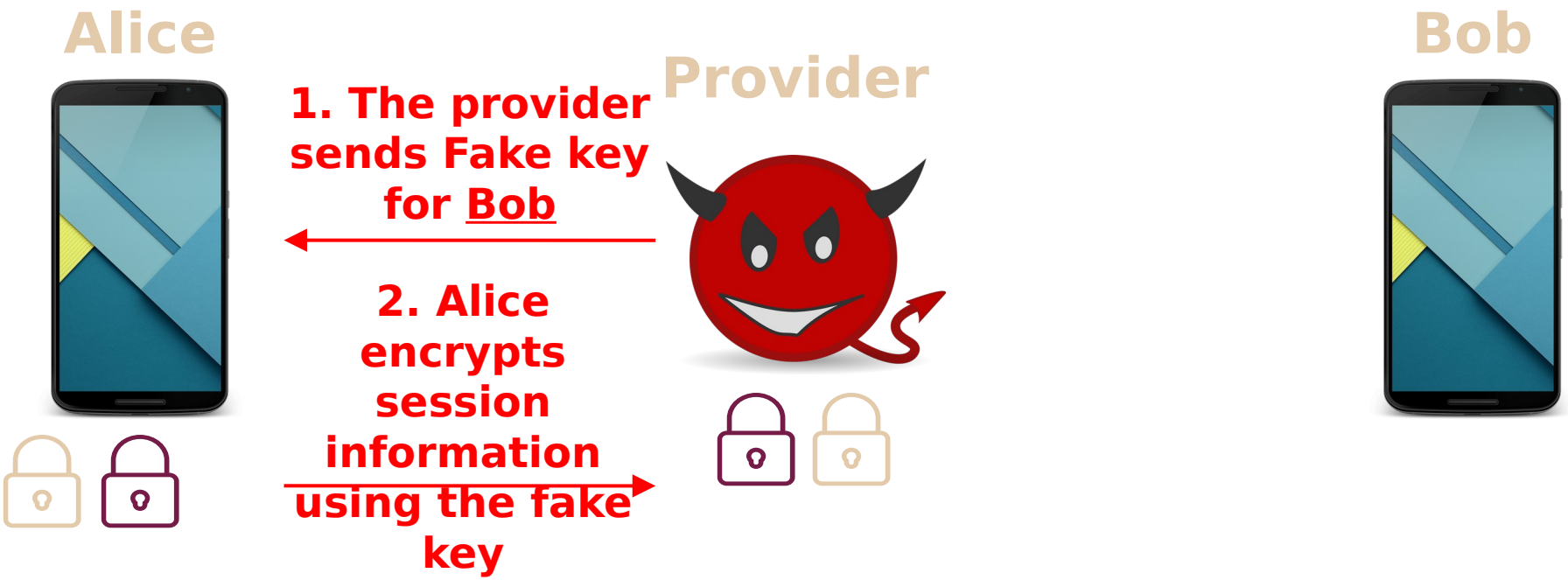


Secure Usability: beyond w

Secure Usability Case Study: Opportunistic End-to-End Encryption



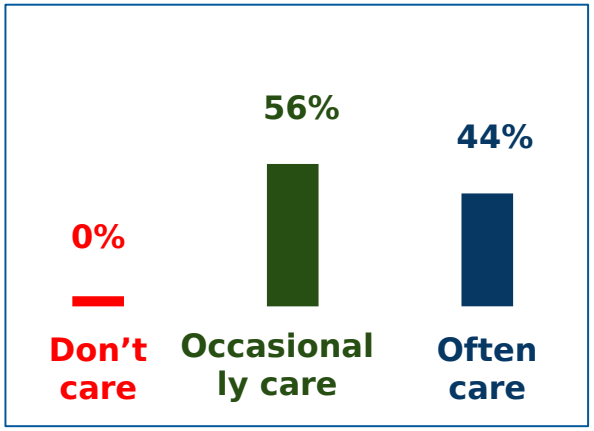
Rogue MitM Provider in Opportunistic E2E Encryption



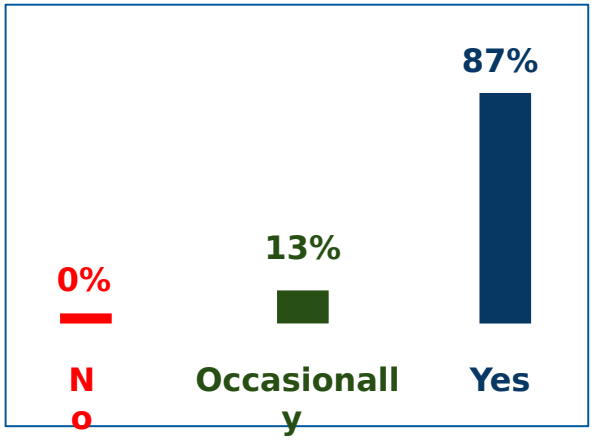
But users did not do authentication!!

User Studies: Privacy

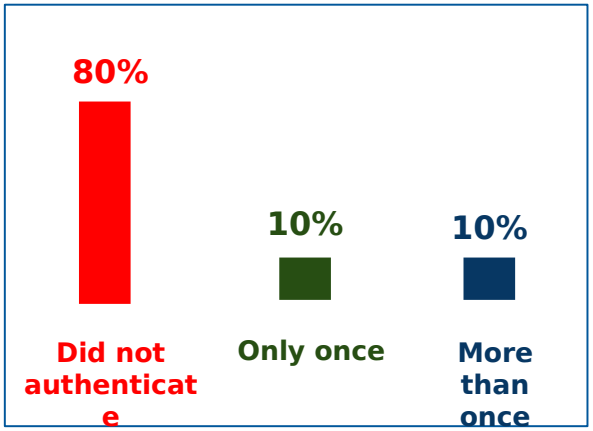
[Herzberg and Leibowitz, "Can Johnny Finally Encrypt? Evaluating E2E-Encryption in Popular IM Applications", 2016]



Do users care about messages privacy?



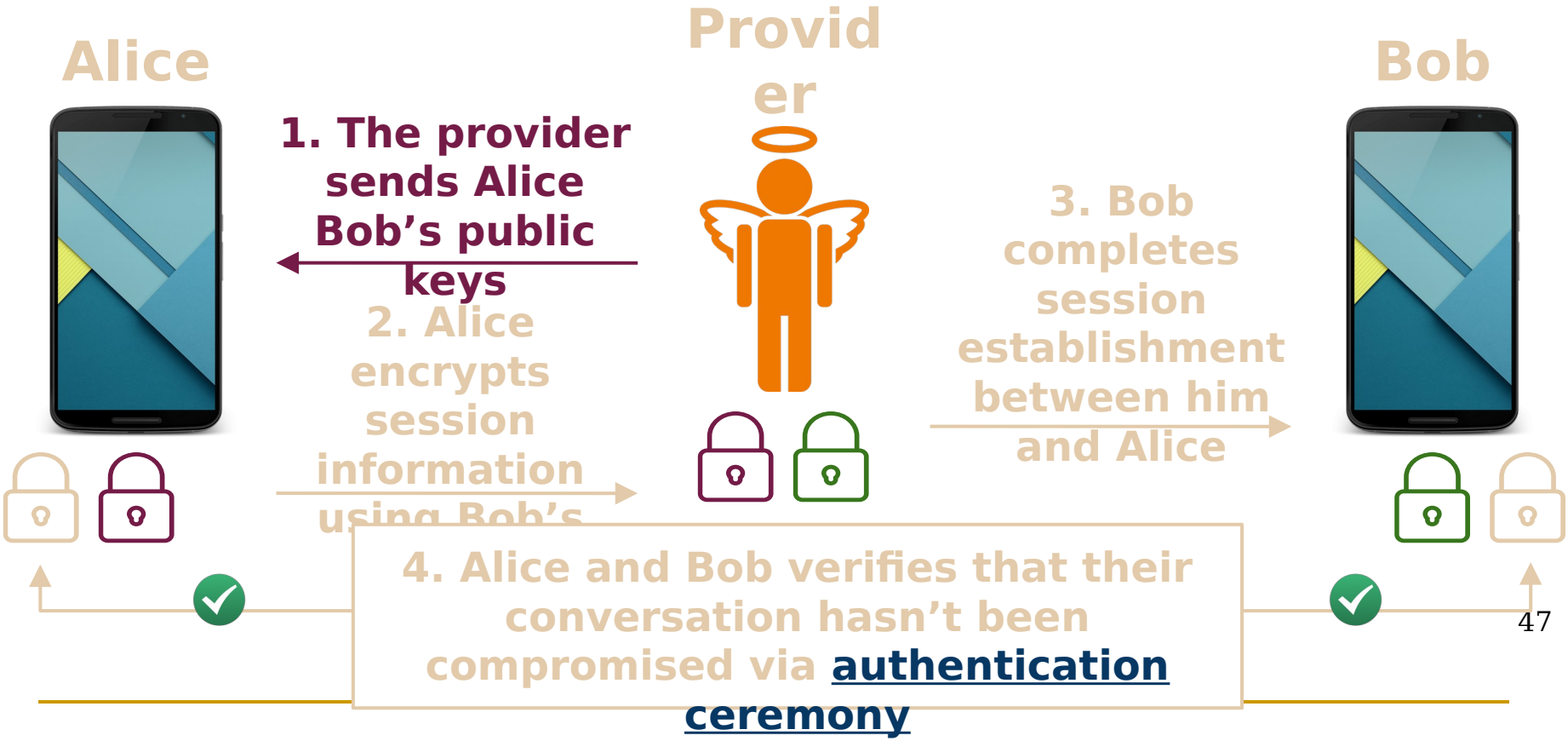
Do users want end-to-end encryption?



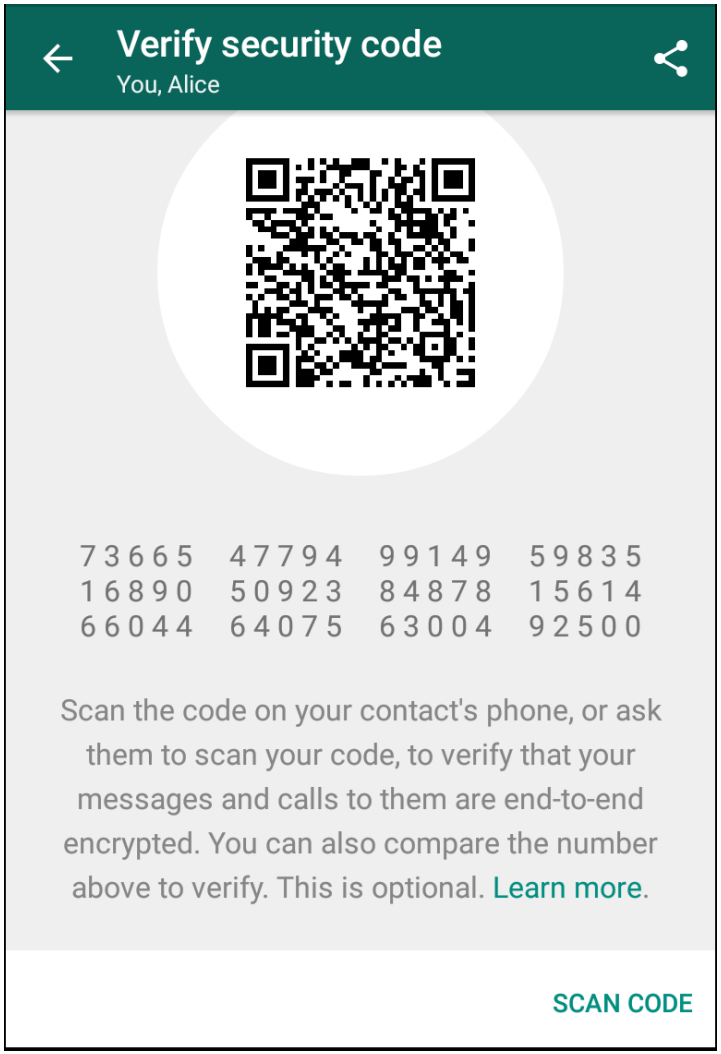
Are users aware of the need to authenticate?

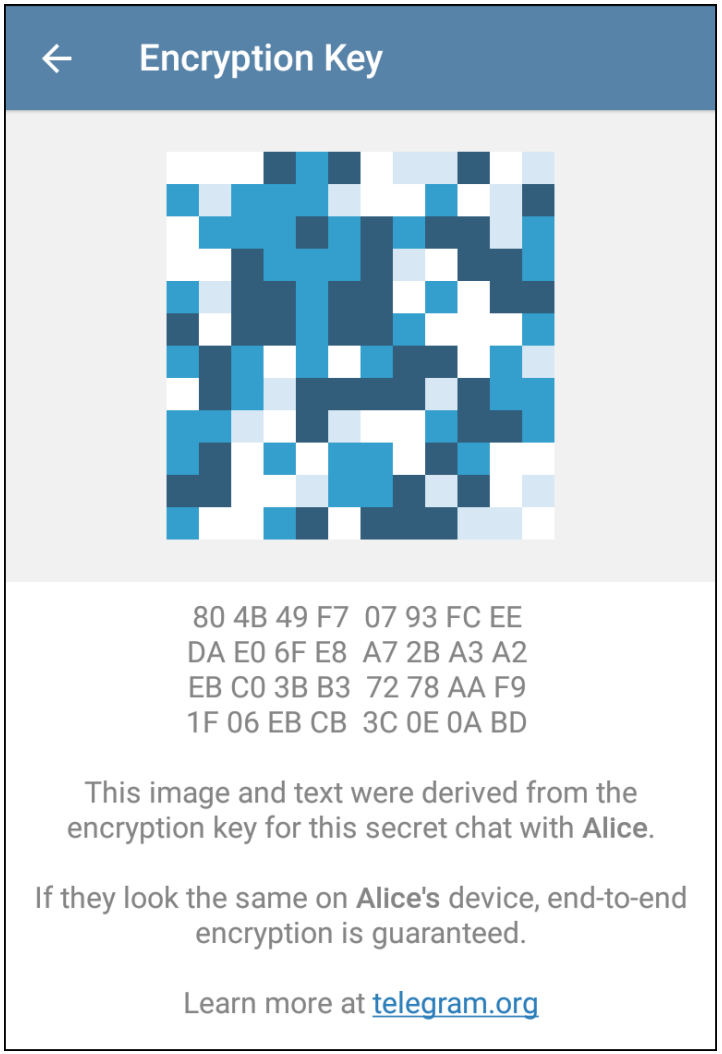
The "privacy paradox"

Authentication Ceremony



Authentication Ceremonies

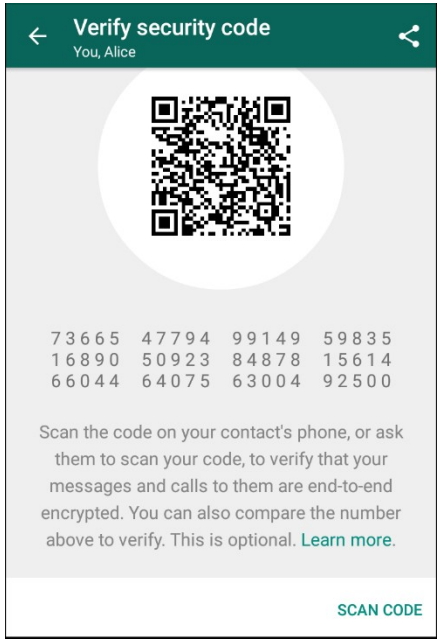


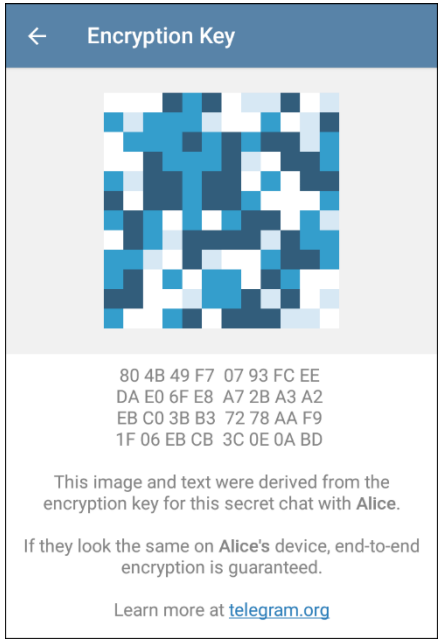


Authentication Ceremonies

What is a reasonable, `minimal' assumption for hashing for this to be secure?

- **CRHF**
- **SPR**
- **Keyed CRHF, with key provided with the image (by provider)**
- **Keyless KDF (extracting randomness)**
- **Random oracle**

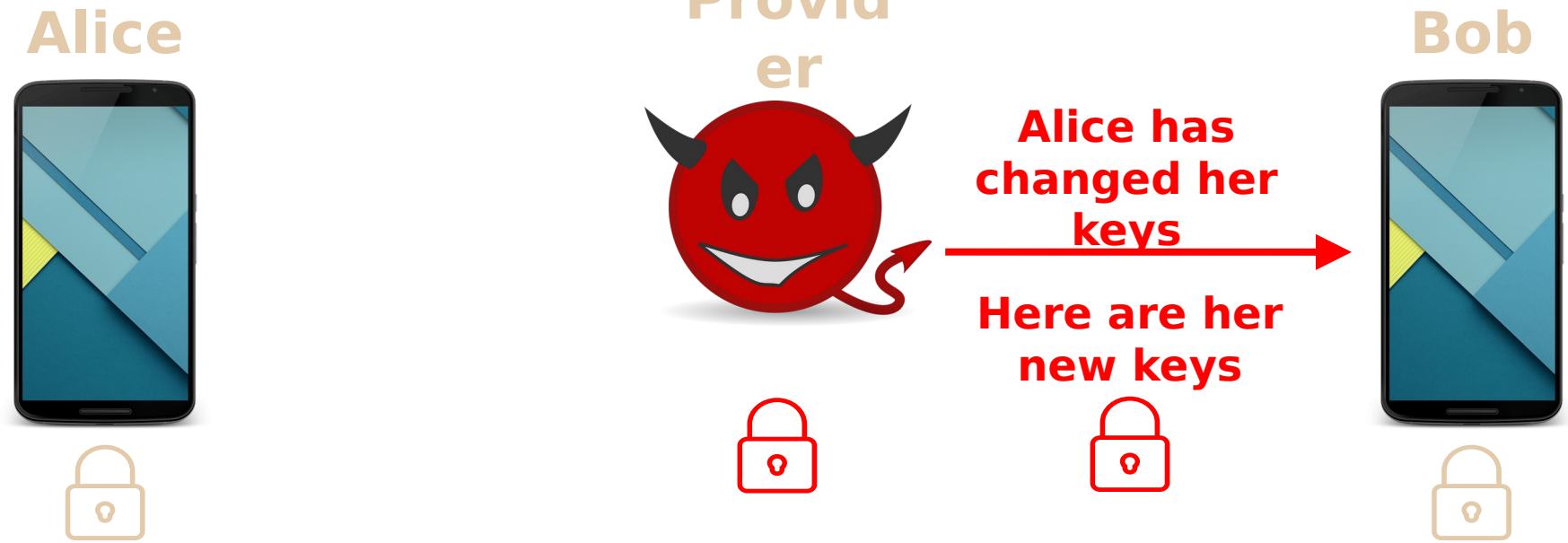




Reality: Authentication isn't Usable

- Even after they learned, <u>most</u> users <u>failed</u> to do it (and they tried hard!)
- Even users that succeeded, were annoyed
  - Hard, time consuming, inconvenient
  - Most said they wouldn't use it
  - Few that said they'll use it… didn't (we checked)
- And… does it really help??

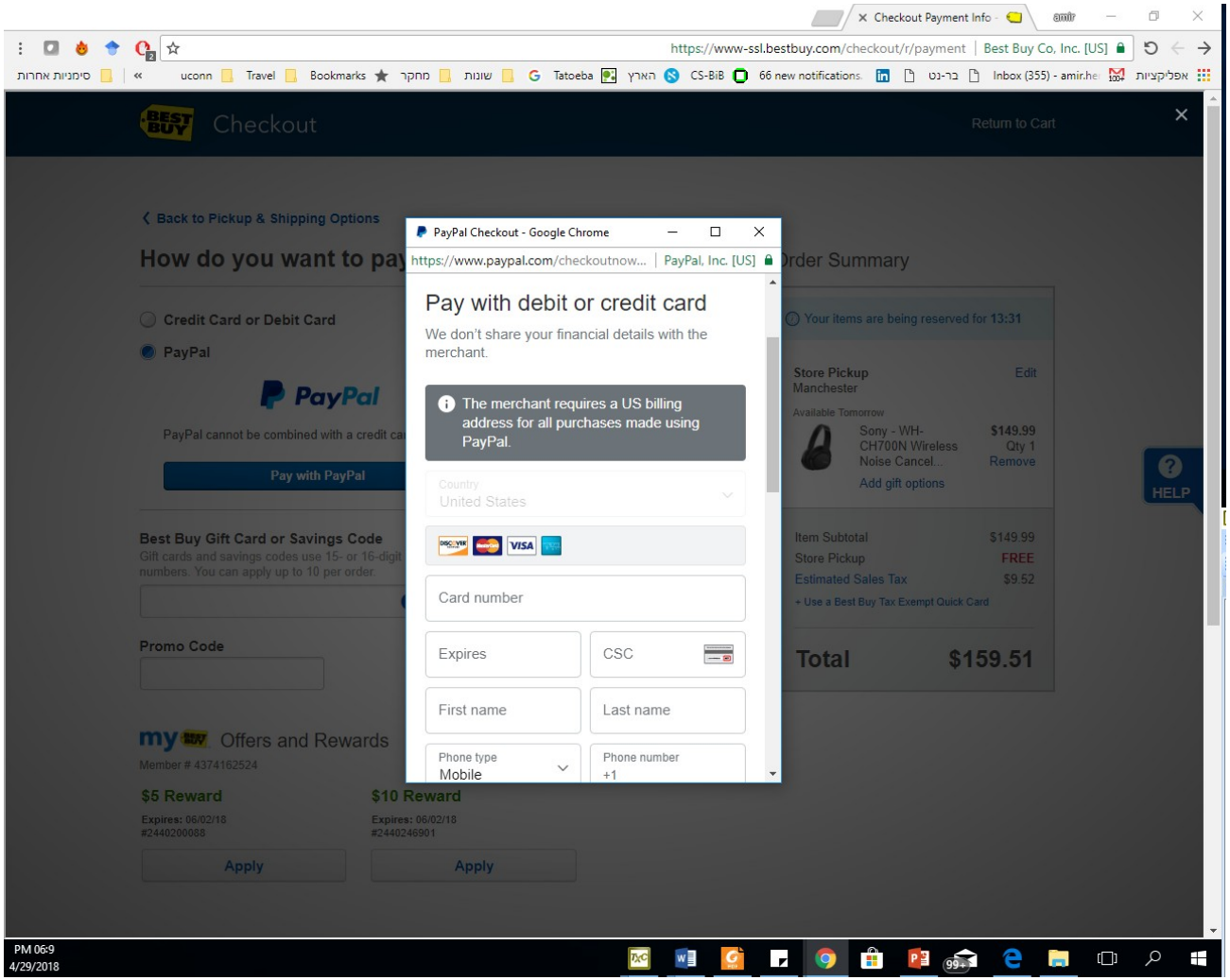
Rogue Provider's 'Key Reset' Even After Authentication



100% success rate!

Summary: Protecting Johnny in the World-Wild-Web

- Usable security: still a huge challenge …
- Robust experimentation is critical:
  - Realistic user behavior Long term, real life
- Less privacy more vulnerable ?
  - Can we ‘teach’ users the value of privacy?
- Challenge: ensuring security while maintaining usability
- Thank you!


Checkout Payment Info
https://www-ssl.bestbuy.com/checkout/r/payment
Best Buy Co, Inc. [US]
Checkout
Return to Cart
Back to Pickup & Shipping Options
How do you want to pay
Credit Card or Debit Card
PayPal
PayPal cannot be combined with a credit ca
Pay with PayPal
Best Buy Gift Card or Savings Code
Promo Code
my Offers and Rewards
Member # 4374162524
$5 Reward
Expires: 06/02/18
#2440200088
Apply
$10 Reward
Expires: 06/02/18
#2440246901
Apply
PayPal Checkout - Google Chrome
https://www.paypal.com/checkoutnow...
PayPal, Inc. [US]
Pay with debit or credit card
We don't share your financial details with the merchant.
The merchant requires a US billing address for all purchases made using PayPal.
Country
United States
Card number
Expires
CSC
First name
Last name
Phone type
Mobile
Phone number
+1
Order Summary
Your items are being reserved for 13:31
Store Pickup
Manchester
Edit
Available Tomorrow
Sony - WH-CH700N Wireless Noise Cancel...
$149.99
Qty 1
Remove
Add gift options
Item Subtotal
$149.99
Store Pickup
FREE
Estimated Sales Tax
$9.52
+ Use a Best Buy Tax Exempt Quick Card
Total
$159.51
HELP
PM 06:9
4/29/2018