UCL

"Protect what people value – and they will value security"

M. Angela Sasse FREng

Professor of Human-Centred Technology

Director, UK Research Institute in Science of Cyber Security

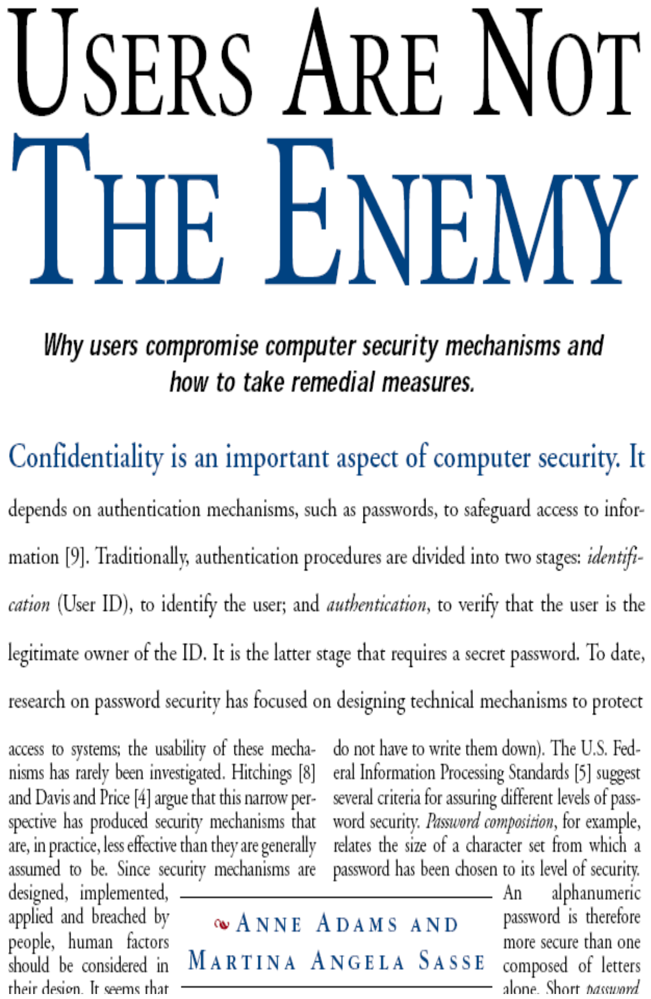
UCL

RISCS

Research Institute in Science of Cyber Security

Background

- Study on escalating cost of password resets in a company
  - – Impossible workload (memory)
  - – Induces workarounds (non-compliance)
  - – Non-compliance → users disbelieve and disrespect security



USERS ARE NOT THE ENEMY

Why users compromise computer security mechanisms and how to take remedial measures.

Confidentiality is an important aspect of computer security. It depends on authentication mechanisms, such as passwords, to safeguard access to information [9]. Traditionally, authentication procedures are divided into two stages: *identification* (User ID), to identify the user; and *authentication*, to verify that the user is the legitimate owner of the ID. It is the latter stage that requires a secret password. To date, research on password security has focused on designing technical mechanisms to protect access to systems; the usability of these mechanisms has rarely been investigated. Hitchings [8] and Davis and Price [4] argue that this narrow perspective has produced security mechanisms that are, in practice, less effective than they are generally assumed to be. Since security mechanisms are designed, implemented, applied and breached by people, human factors should be considered in their design. It seems that

do not have to write them down). The U.S. Federal Information Processing Standards [5] suggest several criteria for assuring different levels of password security. *Password composition*, for example, relates the size of a character set from which a password has been chosen to its level of security. An alphanumeric password is therefore more secure than one composed of letters alone. Short *password*

ANNE ADAMS AND MARTINA ANGELA SASSE

Adams & Sasse CACM 1999

20 years on

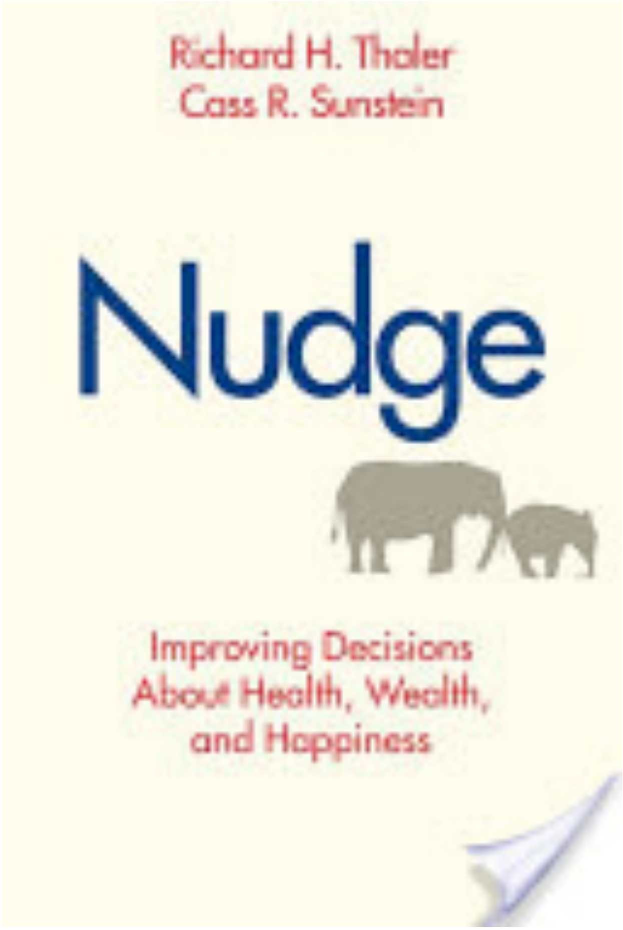
We know that:

1. Complex security causes mistakes
2. High workload security, disruption of and conflicts with primary tasks lead to non-compliance and *shadow security* practices
3. Many security measures have drain user time and effort for little discernable security benefits (e.g. ‘strong’ passwords, SSL warnings, CAPTCHAs)

Categorical imperative of usable security ought to be:
don’t waste user effort and attention, don’t disrupt user activities
C. Herley (2014) *More is not the Answer*. IEEE S&P Magazine.

But there is nagging paternalism in security

- Often justified with ‘nudge’ behavioural economics
- Overlooking that choices have to be genuine, and desirable

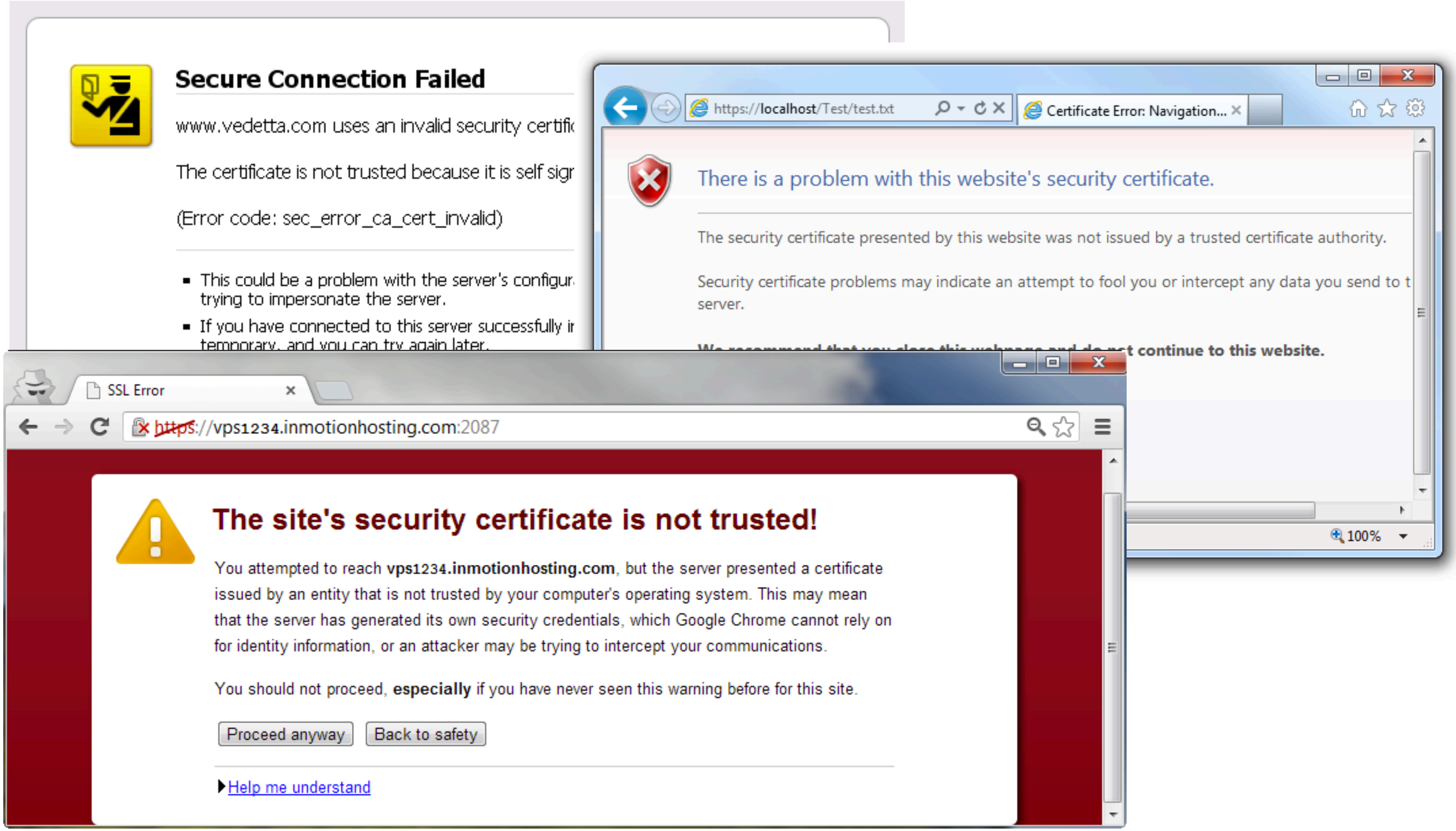


Warnings

- Ignoring of a key usability principle – pop-up dialogue boxes should never be used for common events (Cooper 1995)
- Plus: high false positive rates, plus lack of visibility of consequences – has created habit of swatting and ignoring warnings

Krol et al. (2012): *Don't Work. Can't Work? Why it's time to rethink security warnings*

HTTPS Warnings


https://localhost/Test/test.txt
Certificate Error: Navigation...
100%
SSL Error
https://vps1234.inmotionhosting.com:2087
Proceed anyway
Back to safety
Help me understand

Secure Connection Failed

www.vedetta.com uses an invalid security certifi

The certificate is not trusted because it is self sigr

(Error code: sec_error_ca_cert_invalid)

- This could be a problem with the server's configur trying to impersonate the server.
- If you have connected to this server successfully ir temporary, and you can try again later.

There is a problem with this website's security certificate.

The security certificate presented by this website was not issued by a trusted certificate authority.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to t server.

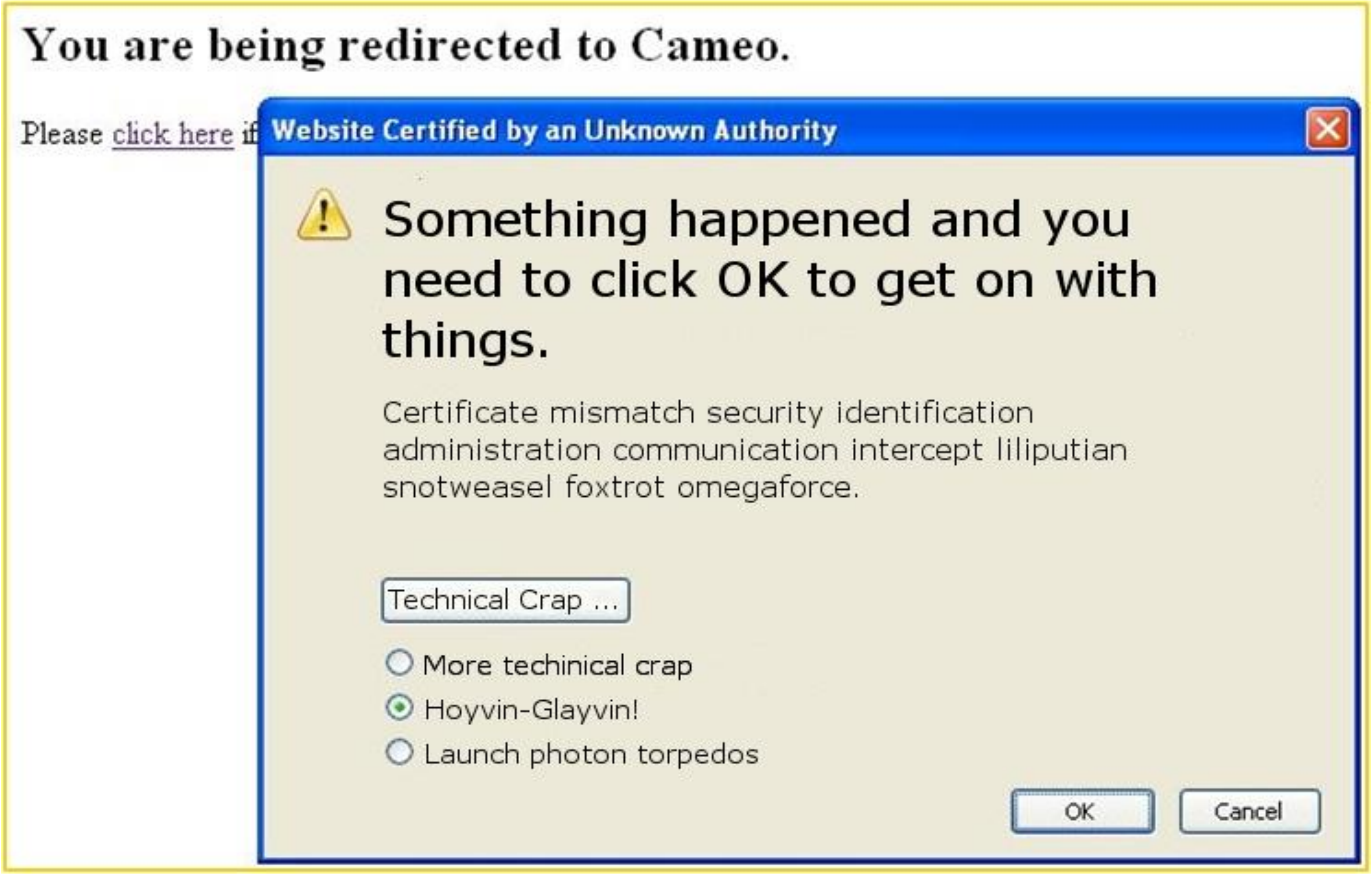
We recommend that you close this webpage and do not continue to this website.

The site's security certificate is not trusted!

You attempted to reach **vps1234.inmotionhosting.com**, but the server presented a certificate issued by an entity that is not trusted by your computer's operating system. This may mean that the server has generated its own security credentials, which Google Chrome cannot rely on for identity information, or an attacker may be trying to intercept your communications.

You should not proceed, **especially** if you have never seen this warning before for this site.

Wh



You are being redirected to Cameo.

Please click here if

Website Certified by an Unknown Authority

Something happened and you need to click OK to get on with things.

Certificate mismatch security identification administration communication intercept liliputian snotweasel foxtrot omegaforce.

○ More techinical crap

● Hoyvin-Glayvin!

○ Launch photon torpedos

Adapted from Jonathan Nightingale

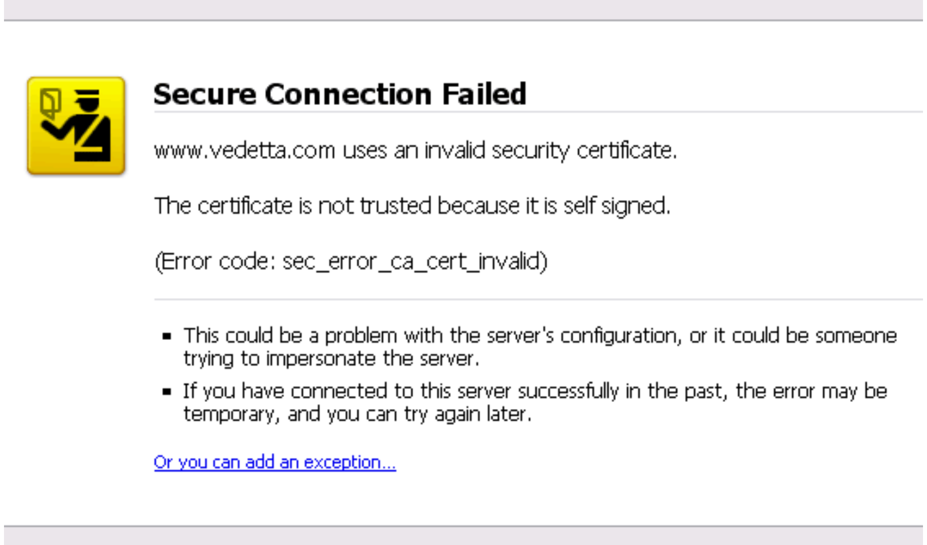
HTTPS: Administrator Mistakes

Akhawe et al. 2013: Server misconfigurations lead to

15.400 per 1

false positive true positive

certificate warnings[1]



Secure Connection Failed

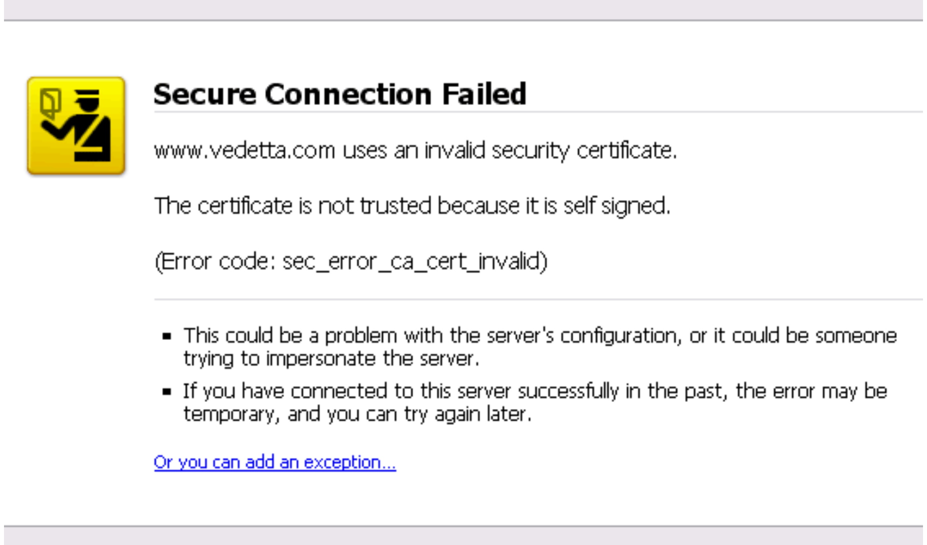
www.vedetta.com uses an invalid security certificate.

The certificate is not trusted because it is self signed.

(Error code: sec_error_ca_cert_invalid)

- This could be a problem with the server's configuration, or it could be someone trying to impersonate the server.
- If you have connected to this server successfully in the past, the error may be temporary, and you can try again later.

Or you can add an exception…



Secure Connection Failed

www.vedetta.com uses an invalid security certificate.

The certificate is not trusted because it is self signed.

(Error code: sec_error_ca_cert_invalid)

- This could be a problem with the server's configuration, or it could be someone trying to impersonate the server.
- If you have connected to this server successfully in the past, the error may be temporary, and you can try again later.

Or you can add an exception…

Trick …

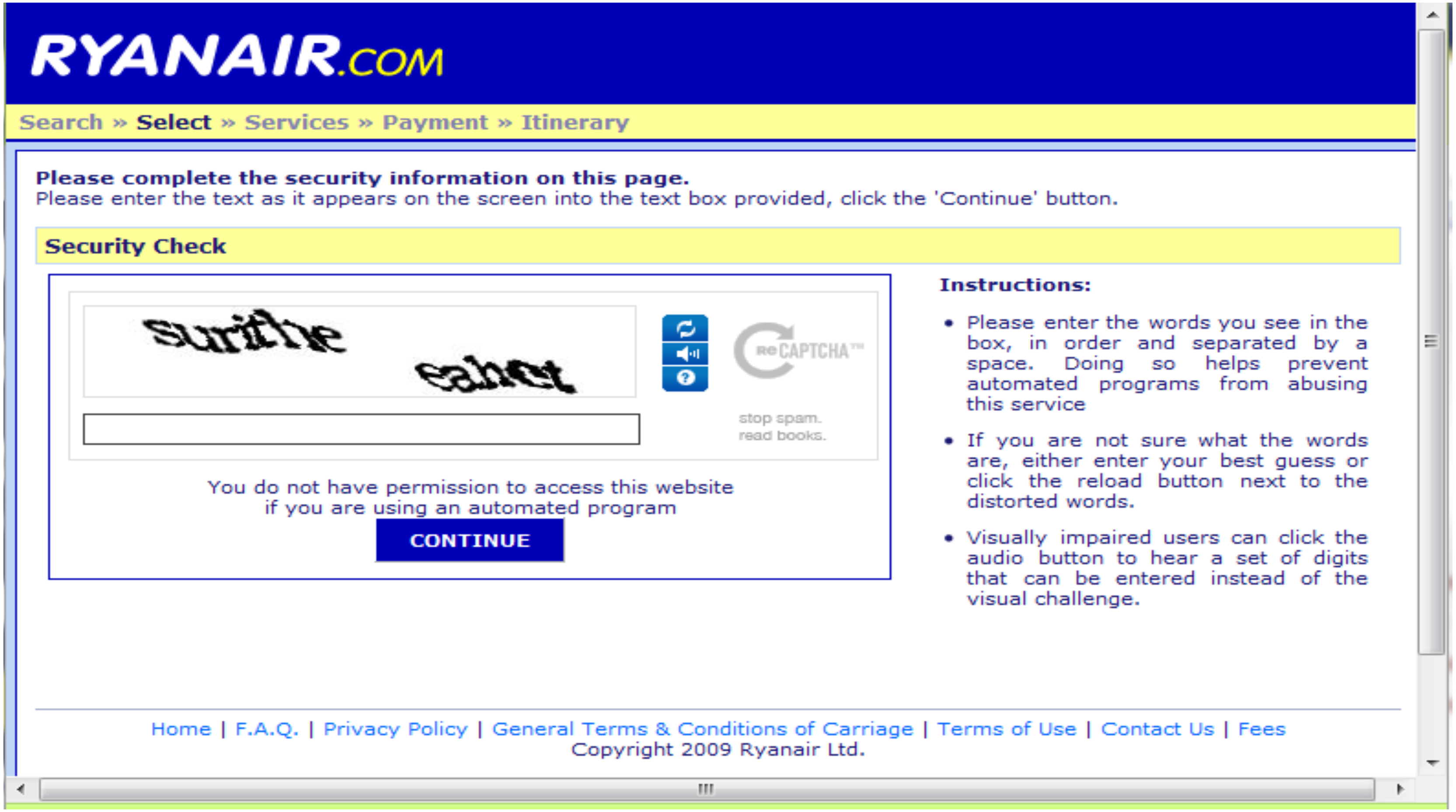
- Felt at al. (2015) applied of recommendations from literature to Chrome SSL warnings
  - keep warnings *brief*
  - use *simple language* to describe *specific risk,* and
  - *illustrate* the potential consequences of going ahead
- Not much improvements
- Next ‘opinonated design’
  - to make it harder for participants to circumvent the warnings.
  - visual design to make the secure course of action look more attractive

… or treat

- Anderson et al. (2015) putting users in fMRI scanner shows brain habituates
- Solution: change design (sizes, colour, text order so users cannot habituate – until 13th view of warning
- What next – electroshocks to force users to pay attention?

CAPTCHAs

- Completely Automated Public Turing test to tell Computers and Humans Apart
- Type of challenge-response test to determine whether the user is human or a bot
- Application areas:
  - Free email account registration
  - Prevent automated guessing attacks
  - Prevent data mining/scraping
  - Prevent manipulation of online data gathering



Please complete the security information on this page.
Please enter the text as it appears on the screen into the text box provided, click the 'Continue' button.

Security Check

You do not have permission to access this website
if you are using an automated program

Instructions:

- Please enter the words you see in the box, in order and separated by a space. Doing so helps prevent automated programs from abusing this service
- If you are not sure what the words are, either enter your best guess or click the reload button next to the distorted words.
- Visually impaired users can click the audio button to hear a set of digits that can be entered instead of the visual challenge.

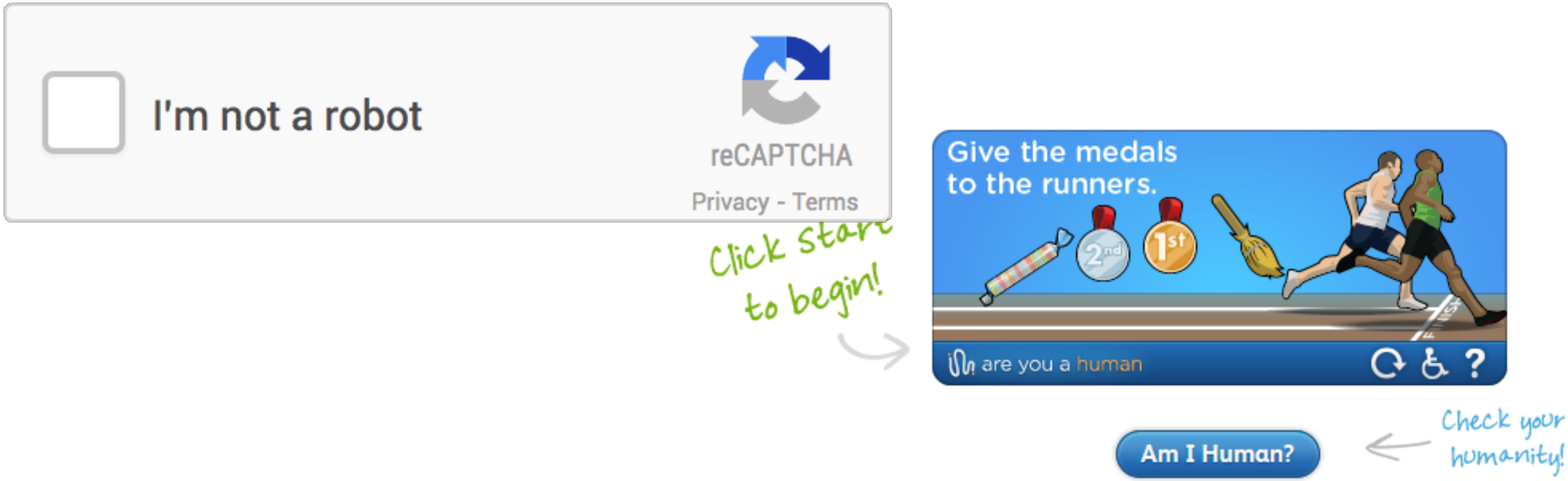
Home | F.A.Q. | Privacy Policy | General Terms & Conditions of Carriage | Terms of Use | Contact Us | Fees

Copyright 2009 Ryanair Ltd.

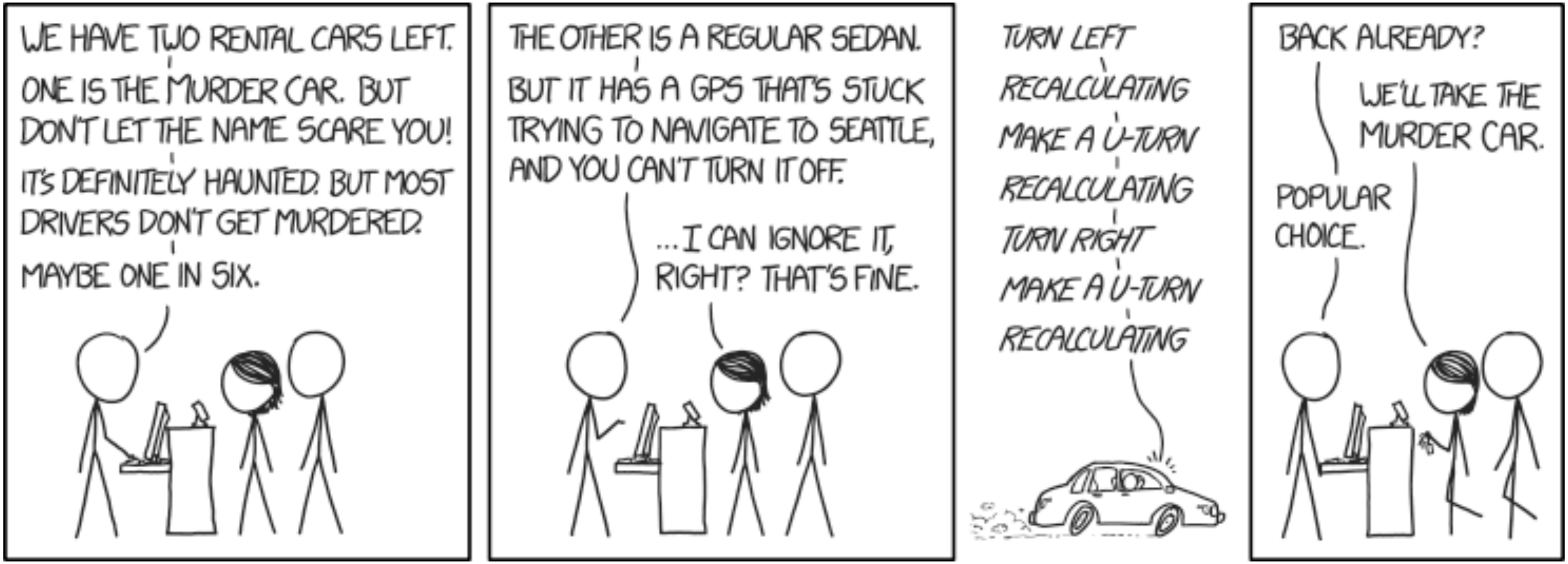
‘Usable’ CAPTCHAs?

- Make users jump through hoops to deal with attacks on service providers, not users themselves
  - *“Don't make users take responsibility for our problems.”* James Edwards

http://www.sitepoint.com/article/captcha-problems-alternatives/



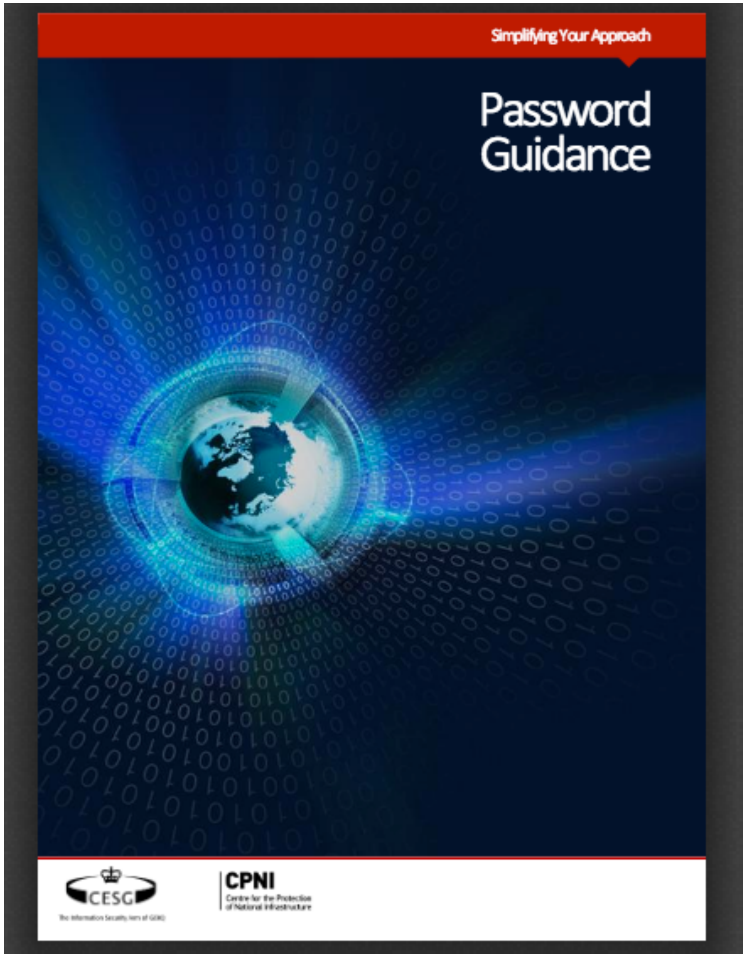
Many security propositions are like this …


WE HAVE TWO RENTAL CARS LEFT.
ONE IS THE MURDER CAR. BUT DON'T LET THE NAME SCARE YOU!
IT'S DEFINITELY HAUNTED. BUT MOST DRIVERS DON'T GET MURDERED.
MAYBE ONE IN SIX.
THE OTHER IS A REGULAR SEDAN.
BUT IT HAS A GPS THAT'S STUCK TRYING TO NAVIGATE TO SEATTLE, AND YOU CAN'T TURN IT OFF.
...I CAN IGNORE IT, RIGHT? THAT'S FINE.
TURN LEFT
RECALCULATING
MAKE A U-TURN
RECALCULATING
TURN RIGHT
MAKE A U-TURN
RECALCULATING
BACK ALREADY?
WE'LL TAKE THE MURDER CAR.
POPULAR CHOICE.

XKCD https://xkcd.com/1837/

Green shoots: new password guidance

- NCSC in the UK, and now NIST in US
- Shift responsibility from users to service providers/system owners
- Realistic demand on individual users



Simplifying Your Approach

Password Guidance

CESG

The Information Security Arm of GCHQ

CPNI

Centre for the Protection of National Infrastructure

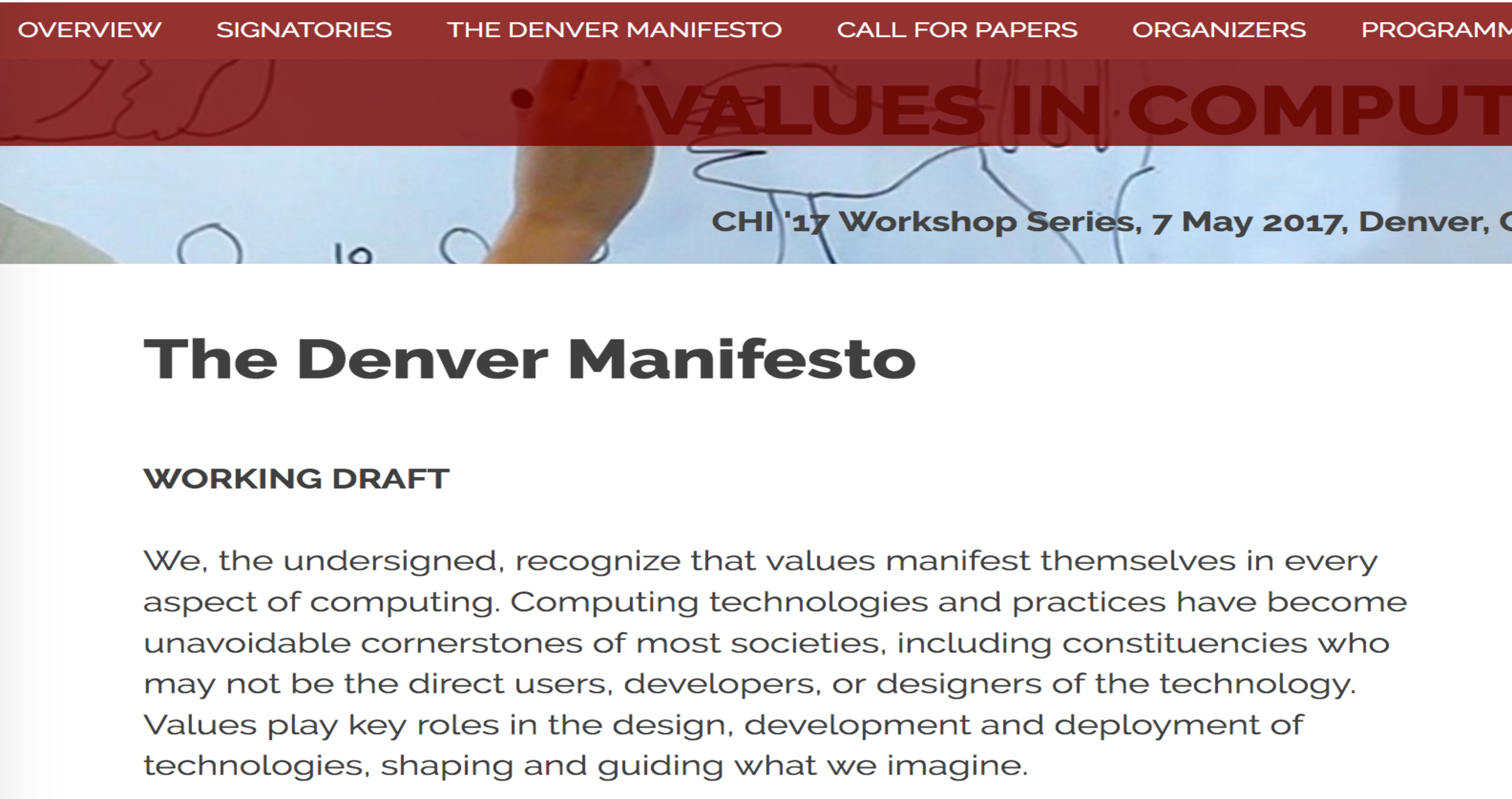
https://www.ncsc.gov.uk/guidance/password-guidance-simplifying-your-approach

Password Guidance: Simplifying Your Approach contains advice for system owners responsible for determining password policy. It is not intended to protect high value individuals using public services. It advocates a dramatic simplification of the current approach at a **systen** level, rather than asking **users** to recall unnecessarily complicated passwords.

More specifically, this document will help you to:

- examine and (if necessary) challenge existing corporate password policies, and argue for a more realistic approach
- understand the decisions to be made when determining password policy
- implement strategies that lessen the workload that complex passwords impose on users
- make your system more secure by suggesting a number of practical steps you can implement

Re-birth of value-based design



The Denver Manifesto

WORKING DRAFT

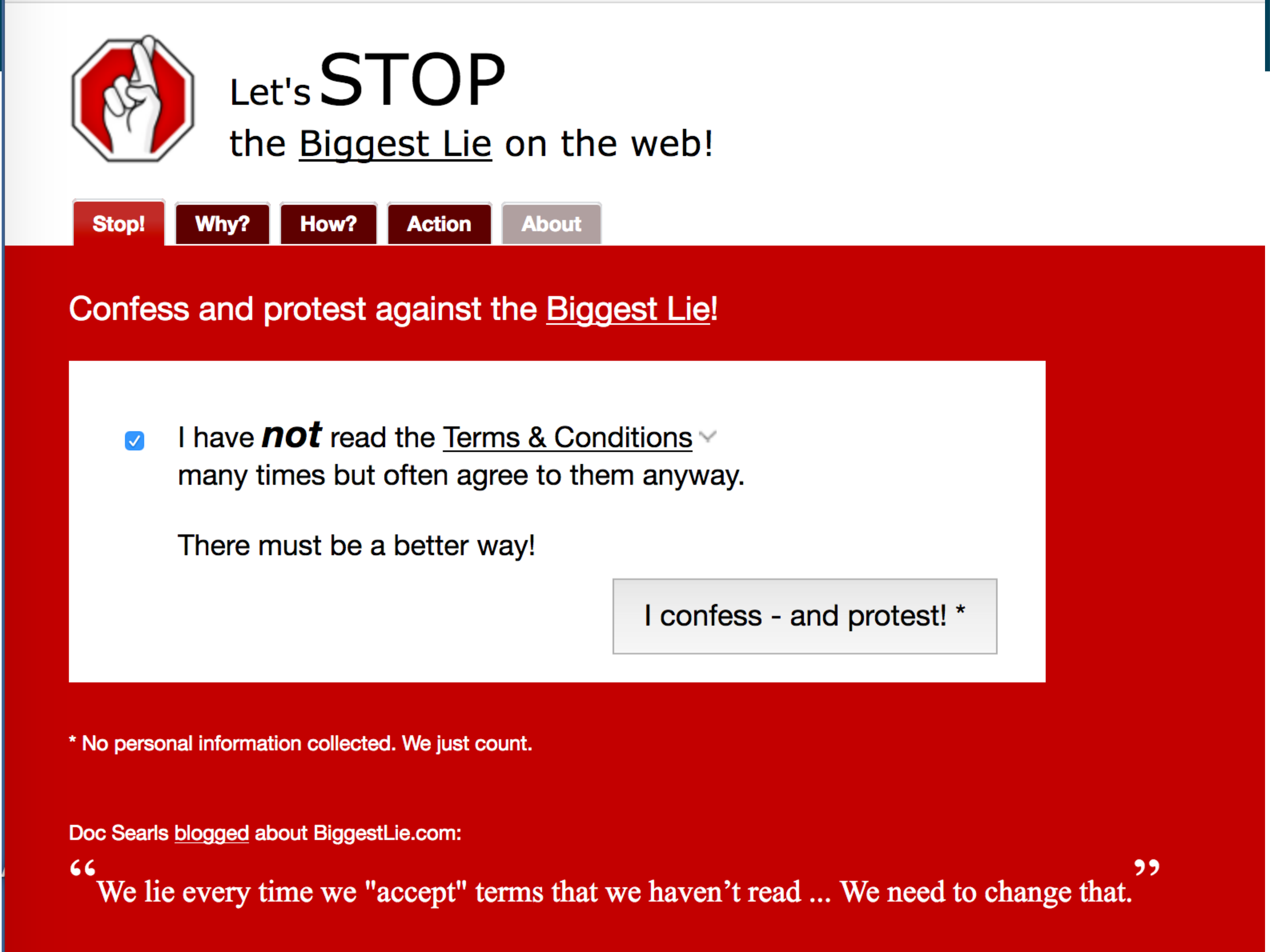
We, the undersigned, recognize that values manifest themselves in every aspect of computing. Computing technologies and practices have become unavoidable cornerstones of most societies, including constituencies who may not be the direct users, developers, or designers of the technology. Values play key roles in the design, development and deployment of technologies, shaping and guiding what we imagine.

“It is important for these values to be explicitly and intentionally considered, not just with respect to the values intended but whose values are included, how conflicting values are negotiated, and how values are instantiated in deployed practice, especially but not solely when a technology is not fully transparent about how it produces its outputs.”

Meaningful consent

1. **Disclosure**: *provide accurate information about benefits and harms*
2. **Comprehension**: *the user must understand what is being disclosed*
3. **Voluntariness**: *user can reasonably resist participation*
4. **Competence**: *user has mental, emotional and physical competences to give informed consent*
5. **Agreement**: *clear opportunity to accept or decline*
6. **Minimal Distraction**: *user's attention should not be diverted from main task*

B. Friedmann, P. Lin & J. K. Miller: Informed Consent by Design
In Cranor & Garfinkel eds. Security and Usability 2005



Let's STOP the Biggest Lie on the web!

Confess and protest against the Biggest Lie!

☑ I have ***not*** read the Terms & Conditions many times but often agree to them anyway.

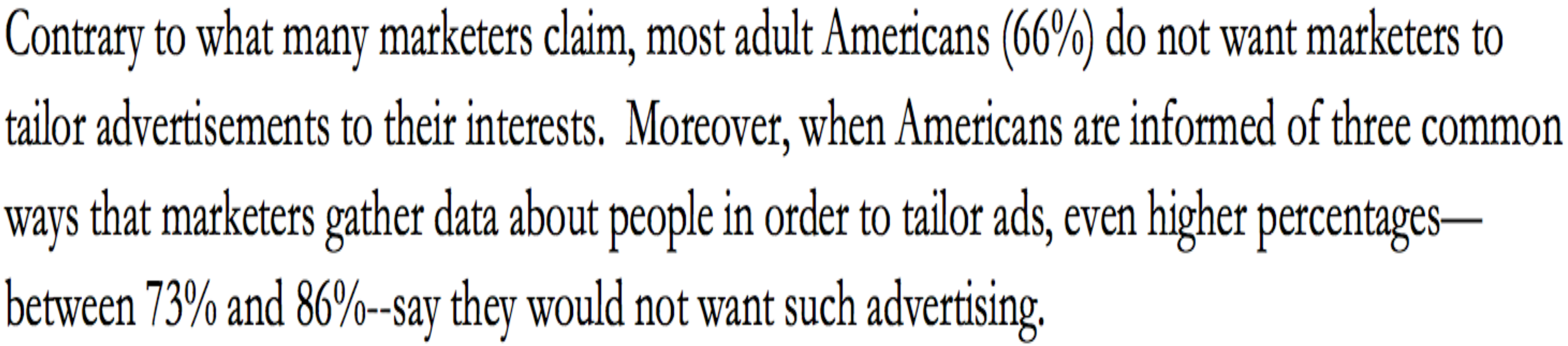
There must be a better way!

* No personal information collected. We just count.

Doc Searls blogged about BiggestLie.com:

> “We lie every time we "accept" terms that we haven’t read ... We need to change that.”

People do value privacy



Contrary to what many marketers claim, most adult Americans (66%) do not want marketers to tailor advertisements to their interests. Moreover, when Americans are informed of three common ways that marketers gather data about people in order to tailor ads, even higher percentages—between 73% and 86%--say they would not want such advertising.

Turow et al. (2015)*:* Electronic copy available at: http://ssrn.com/abstract=1478214

“Why Johnny Can’t Encrypt”

- Whitten & Tygar (1999) Graphical UI to PGP 5.0
- Only 2/12 participants managed to complete task of generating keys, sending encrypted and decrypting received messages; some who sent plain text thought they had encrypted them!

Solution?

- Alma Whitten created the LIME tutorial to educate users about public key cryptography

"There are significant benefits to supporting users in developing a certain base level in generalizable security knowledge. A user who knows that, regardless of what application is in use, one kind of tool protects the privacy of transmission, a second kind protects the integrity of transmission, and a third kind protects the access to local resources, is much more empowered than one who must start afresh with each application."

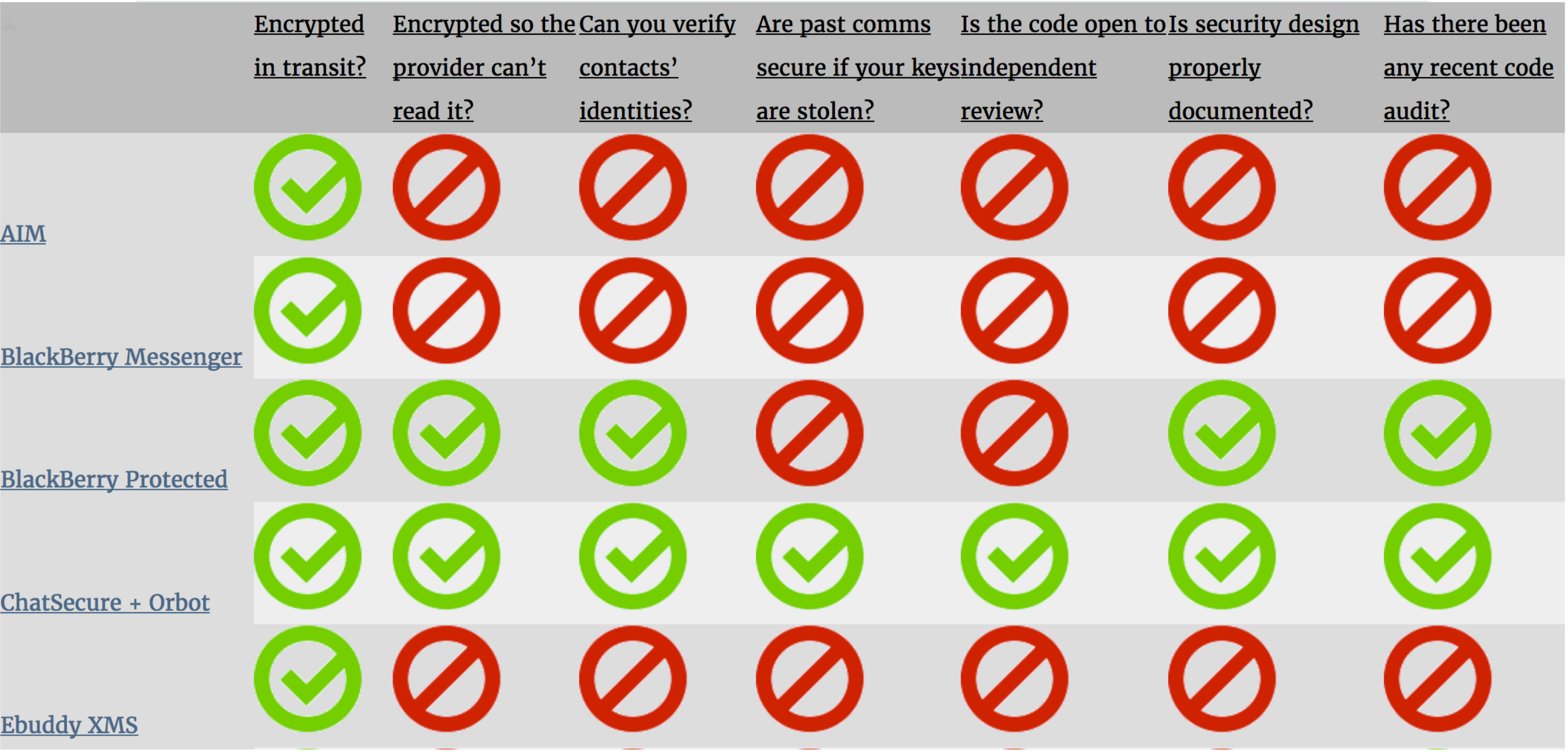
www.gaudior.net/**alma**/MakingSecurityUsable.pdf

A telling observation …

“*… when presented with a software programme incorporating visible public key cryptography, users often complained during the first 10-15 minutes of the testing that they would expect* ‘that sort of thing’ *to be handled invisibly. As their exposure to the software continued and their understanding of the security mechanism grew, they generally ceased to make that complaint.*”

Clear expression of what users (don’t) want –
Overruled by well-meaning paternalism

EFF scorecard criteria don’t match users’



	Encrypted in transit?	Encrypted so the provider can’t read it?	Can you verify contacts’ identities?	Are past comms secure if your keys are stolen?	Is the code open to independent review?	Is security design properly documented?	Has there been any recent code audit?
AIM	✓	⊘	⊘	⊘	⊘	⊘	⊘
BlackBerry Messenger	✓	⊘	⊘	⊘	⊘	⊘	⊘
BlackBerry Protected	✓	✓	✓	⊘	⊘	✓	✓
ChatSecure + Orbot	✓	✓	✓	✓	✓	✓	✓
Ebuddy XMS	✓	⊘	⊘	⊘	⊘	⊘	⊘

“People want to protect themselves, not join a crypto-cult.”

Philip Hallam-Baker at PKI Workshop 2006

Encrypted tools today

Ruba Abu-Salma (UCL) interviewed 60 users of chat – all had tried to use encrypted chat tools, but most stopped using them

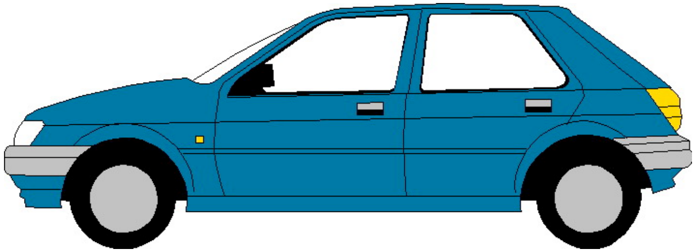
1. Lack of utility
2. Usability problems
3. Misconceptions - about risks, and protection offered by the tools

R Abu-Salma paper at IEEE S&P this week!

Utility

1. Primary task = communication = need to be able to reach your intended communication partner
2. Or partners – secure tools don’t support group chat

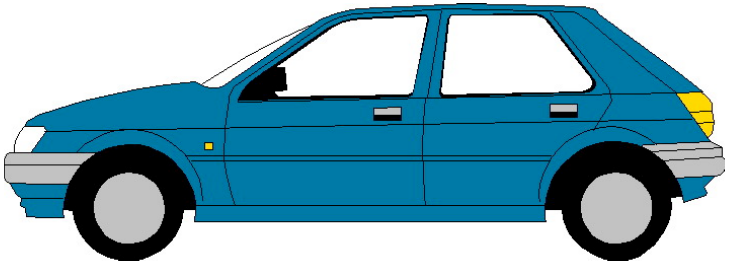
if the chat tool was a car …



Usability

1. Many tools have installation problems
2. Key exchange is cumbersome
3. Some are slow to decrypt (e.g. *Threema*)

If the chat tool was a car …



Example 2: Sandboxing

- In desktop environments, does not support how users work
- Reduces functionality because data cannot be moved to where it is needed
- On the other hand – does not support keeping different project/clients’ data separate.
- So users disable sandboxing, sooner or later

S. Dodier et al.: No Good Reason to Remove Features:
Expert Users Value Useful Apps over Secure Ones. Procs HCII 2017

Less benign paternalism

"Not only in security is it the case that an ordinary person has a problem and a friendly mathematician solves a neighbouring problem. An example that is of interest here is the electronic book. We have a pretty good idea of the semantics of the paper book. We go and buy it, we can lend it to our spouse or to a friend, we can sell it, we can legitimately copy small bits of it for our own use, and so on."

R. Needham: Computer security? The Clifford Paterson Lecture, 2002. http://rsta.royalsocietypublishing.org/

Back to Denver Manifesto

“As a long-term strategy to improve practices in industry and academia, we believe educational programs in computer science and adjacent fields should include focused attention to the values intertwined with the other aspects of career preparation for the field. This training should provide students with the tools necessary for discussing and evaluating relevant values and tensions between them. In addition to providing tools for assessing and communicating about direct impacts, this education should foster an understanding of indirect externalities and risk evaluation, without equating risks with harms.”

“It should prepare students to think critically, reflectively, and empathetically. It should prepare students to integrate diverse perspectives, and understand the cultural and historical contexts that shape present conditions. It should provide students with an understanding of how responsibility for creating products and systems that instantiate values may be distributed. It is a moral imperative for upstanding individuals in this field not to abdicate responsibility for the values manifest in the products of their work, or those espoused in their work environment.”

Or as Jean-Luc would put it:

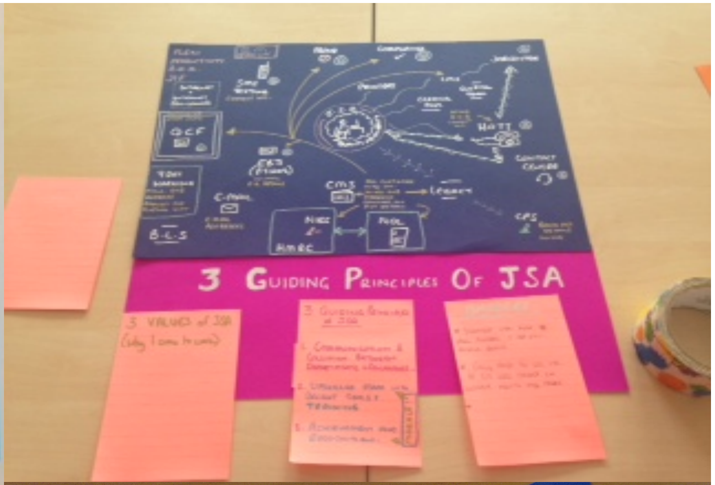
Department of Work and Pensions

Engagement case study Lizzie Coles-Kemp (RHUL) and colleagues on the Cyber Security Cartographies project

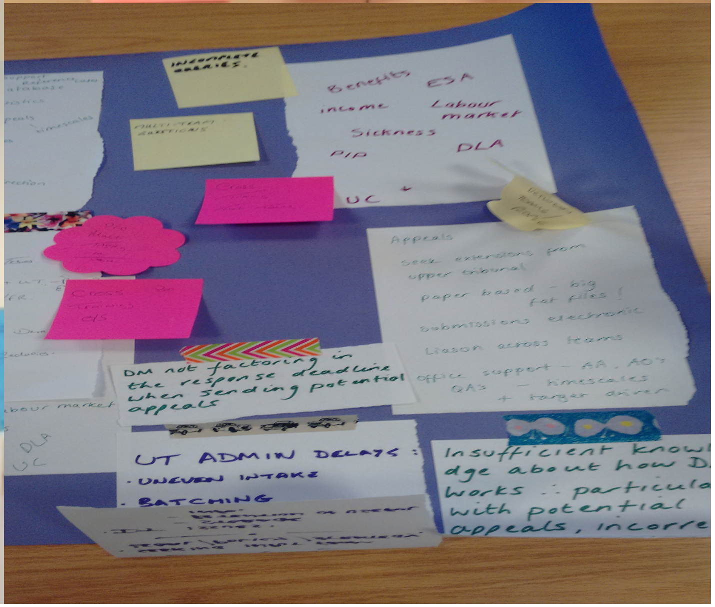
Case Study Programme

- The following objectives were agreed:
  - Help develop understanding of the target audiences for the Department’s information protection policies;
  - Further develop the messaging around the Department’s information protection policies and compliance.
- It was agreed that the case study programme would:
  - Develop a series of user stories in cartoon form that depict the wider challenges faced by different elements of the delivery chain when trying to comply with information protection policies;
  - Produce narrative outputs that can also used for training and education programmes;
  - Present methods that can re-used as part of information governance activities within the Department.

VISITS
EMAIL
RM
MORTGAGE/THIRD PARTY
ESA NEW CLAIMS
NT FORMS PORTAL
LEGACY
CAM
FRAUD REFERRAL
CIS
DWT
DMACC
CMS
HOT
(GMS) HTE
INTERLINE
TRACKER
LMS
CPS
NILS
JIF
CLIENT ZONE
MSRS
CUSTOMER INFORMATION
STAFF INFORMATION
What is security?
Good Customer Service


QCF
CMS
C-MAIL
LEGACY
B.L.S
HMRC
CPS
HOTT
3 GUIDING PRINCIPLES OF JSA
3 VALUES of JSA
3 Guiding Principles of JSA

CHALLENGES
AND
BARRIERS

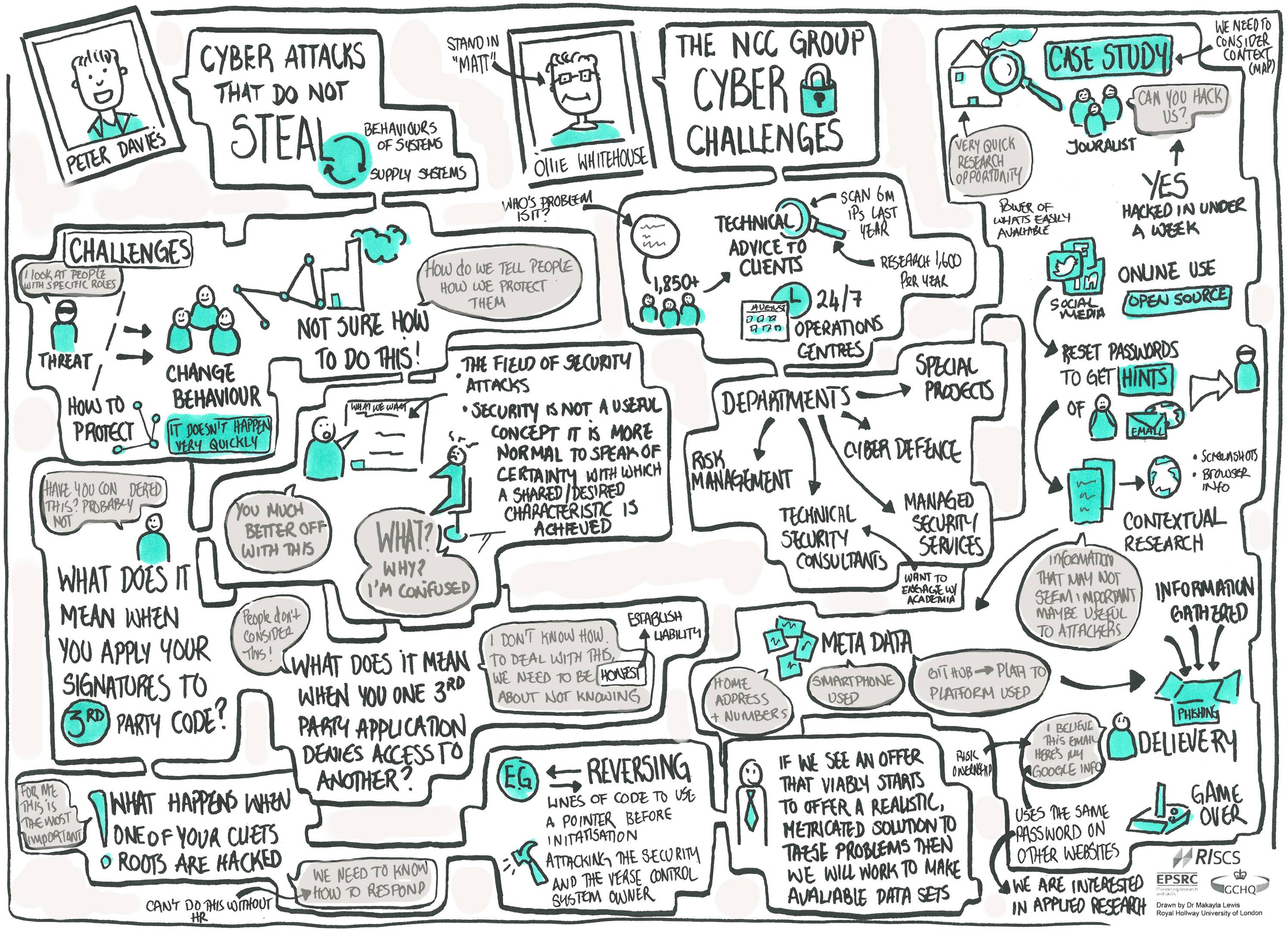

INCOMPLETE ENQUIRIES
Benefits
ESA
income
Labour market
Sickness
PIP
DLA
UC
Appeals
seek extensions from upper tribunal
paper based - big fat files!
submissions electronic
Liason across teams
office support - AA, AO's
OA's - timescales + target driven
DM not factoring in the response deadline when sending potential appeals
UT ADMIN DELAYS:
· UNEVEN INTAKE
· BATCHING
Insufficient knowledge about how D. works ∴ particular with potential appeals, incorre

What we learned

- Collaboration
  - An important means of improving security control strength and overcoming some of the problems that are a factor in real world environments (e.g. legacy IT and a complex regulatory environment)
- Human sign-posting
  - Implications of organisational restructure and centralisation
- Rapport building
  - Process restructure that removes or reduces face-to-face engagement either between service providers and service users or internally between service provider teams increases the likelihood of risks to the confidentiality, availability and integrity of information in a variety of ways.

RISCS

Research Institute in Science of Cyber Security


PETER DAVIES
CYBER ATTACKS THAT DO NOT STEAL
BEHAVIOURS OF SYSTEMS
SUPPLY SYSTEMS
STAND IN "MATT"
OLLIE WHITEHOUSE
THE NCC GROUP CYBER CHALLENGES
CASE STUDY
WE NEED TO CONSIDER CONTEXT (MAP)
CAN YOU HACK US?
JOURNALIST
VERY QUICK RESEARCH OPPORTUNITY
POWER OF WHATS EASILY AVAILABLE
YES
HACKED IN UNDER A WEEK
CHALLENGES
I LOOK AT PEOPLE WITH SPECIFIC ROLES
THREAT
CHANGE BEHAVIOUR
HOW TO PROTECT
IT DOESN'T HAPPEN VERY QUICKLY
NOT SURE HOW TO DO THIS!
HOW DO WE TELL PEOPLE HOW WE PROTECT THEM
WHO'S PROBLEM IS IT?
TECHNICAL ADVICE TO CLIENTS
SCAN 6M IPs LAST YEAR
RESEARCH 1,600 PER YEAR
1,850+
AUGUST
24/7 OPERATIONS CENTRES
SOCIAL MEDIA
ONLINE USE
OPEN SOURCE
RESET PASSWORDS TO GET HINTS OF
EMAIL
THE FIELD OF SECURITY ATTACKS
• SECURITY IS NOT A USEFUL CONCEPT IT IS MORE NORMAL TO SPEAK OF CERTAINTY WITH WHICH A SHARED/DESIRED CHARACTERISTIC IS ACHIEVED
WHAT WE WANT
YOU MUCH BETTER OFF WITH THIS
WHAT? WHY? I'M CONFUSED
DEPARTMENTS
SPECIAL PROJECTS
CYBER DEFENCE
RISK MANAGEMENT
TECHNICAL SECURITY CONSULTANTS
MANAGED SECURITY SERVICES
WANT TO ENGAGE W/ ACADEMIA
• SCREENSHOTS
• BROWSER INFO
CONTEXTUAL RESEARCH
HAVE YOU CONSIDERED THIS? PROBABLY NOT
WHAT DOES IT MEAN WHEN YOU APPLY YOUR SIGNATURES TO 3RD PARTY CODE?
PEOPLE DON'T CONSIDER THIS!
WHAT DOES IT MEAN WHEN YOU ONE 3RD PARTY APPLICATION DENIES ACCESS TO ANOTHER?
I DON'T KNOW HOW TO DEAL WITH THIS, WE NEED TO BE HONEST ABOUT NOT KNOWING
ESTABLISH LIABILITY
META DATA
HOME ADDRESS + NUMBERS
SMARTPHONE USED
GIT HUB → PLATH TO PLATFORM USED
INFORMATION THAT MAY NOT SEEM IMPORTANT MAYBE USEFUL TO ATTACKERS
INFORMATION GATHERED
PHISHING
DELIEVERY
I BELIEVE THIS EMAIL HERE'S MY GOOGLE INFO
RISK OWNERSHIP
FOR ME THIS IS THE MOST IMPORTANT
WHAT HAPPENS WHEN ONE OF YOUR CLIETS ROOTS ARE HACKED
WE NEED TO KNOW HOW TO RESPOND
CAN'T DO THIS WITHOUT HR
E.G. REVERSING
LINES OF CODE TO USE A POINTER BEFORE INITIATISATION
ATTACKING THE SECURITY AND THE VERSE CONTROL SYSTEM OWNER
IF WE SEE AN OFFER THAT VIABLY STARTS TO OFFER A REALISTIC, METRICATED SOLUTION TO THESE PROBLEMS THEN WE WILL WORK TO MAKE AVAILABLE DATA SETS
GAME OVER
USES THE SAME PASSWORD ON OTHER WEBSITES
WE ARE INTERESTED IN APPLIED RESEARCH
RISCS
EPSRC
GCHQ
Drawn by Dr Makayla Lewis
Royal Holloway University of London

The need for engagement with staff and citizen-clients

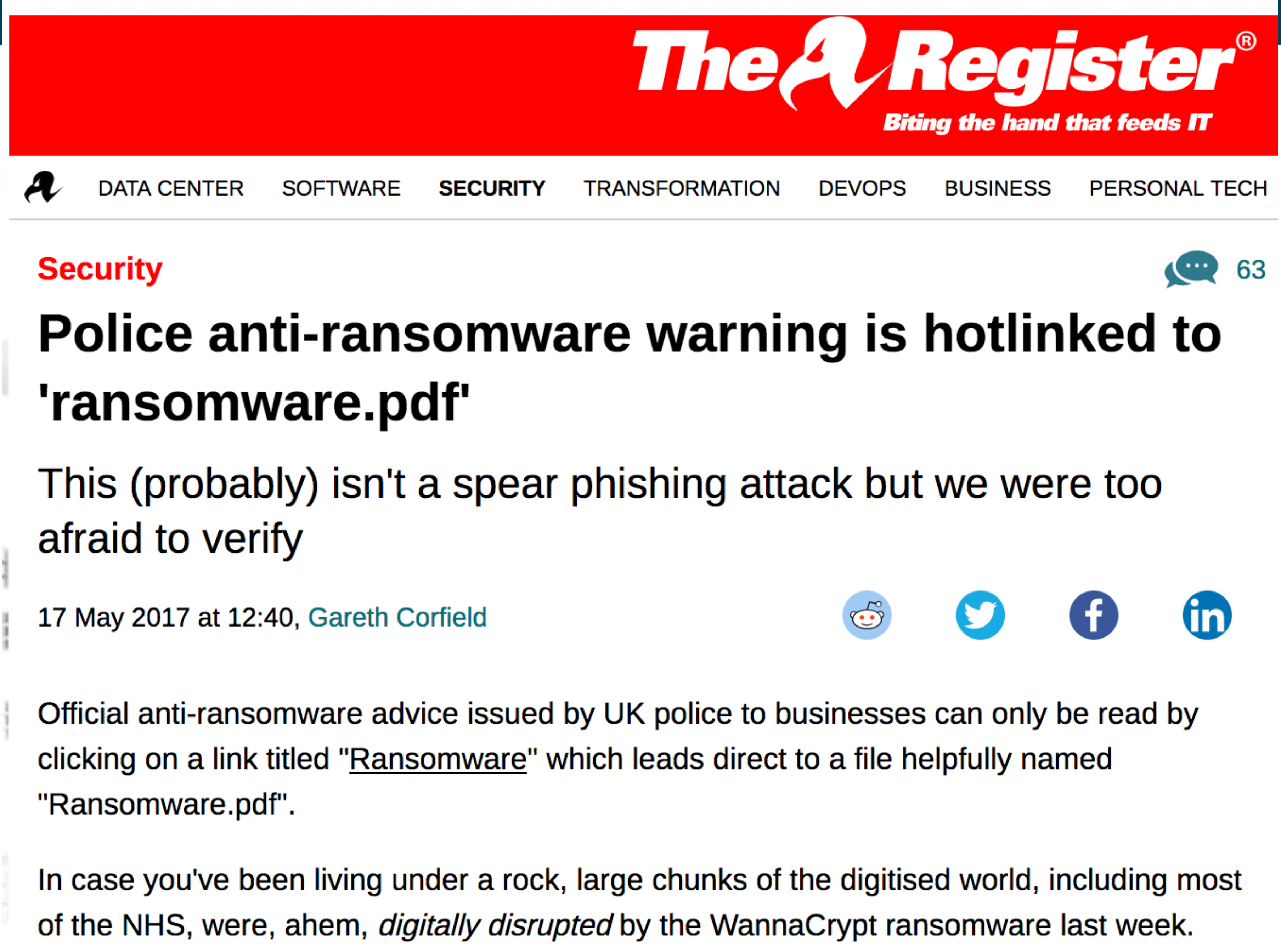
- real-world security problems are complex, need interaction to tease apart
- *“the term ‘security’ is not a useful concept– it is more normal to speak of certainty within a shared/ desired characteristic is achieved.”*
  - Real-world security research requires an understanding of what is of *value* to a particular community
  - Behaviour change takes time. “*It doesn’t happen very quickly*”
  - Often, underlying cause is outdated and/or badly configured IT!

Something we have witnessed just now …

- Final example: ‘security awareness’ that just wastes users time, bad advice

“We urge you to be vigilant and not to open emails that are unexpected, unusual or suspicious in any way. If you experience any unusual computer behaviour, especially any warning messages, please contact your IT support immediately and do not use your computer further until advised to do so.”

UCL IT Department



Security

Police anti-ransomware warning is hotlinked to 'ransomware.pdf'

This (probably) isn't a spear phishing attack but we were too afraid to verify

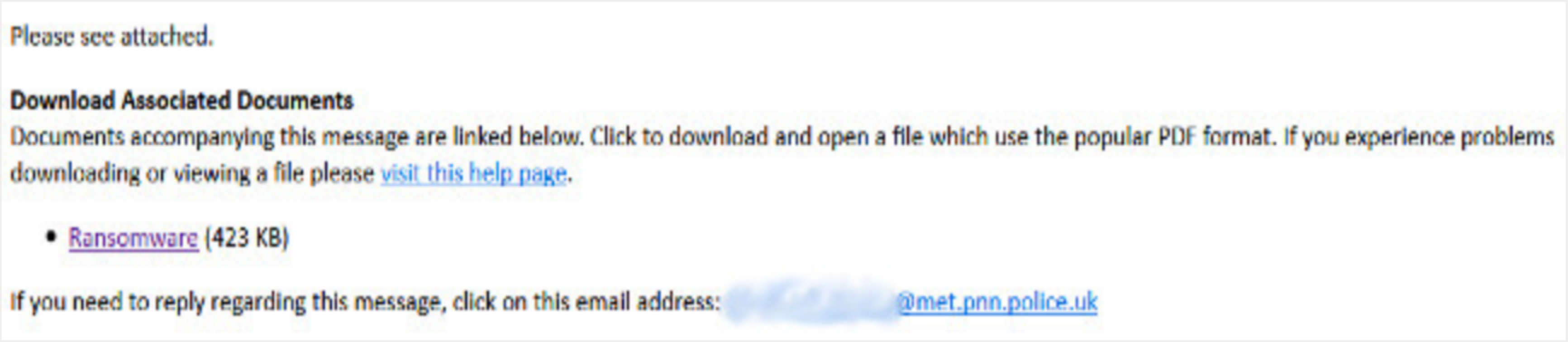
17 May 2017 at 12:40, Gareth Corfield

Official anti-ransomware advice issued by UK police to businesses can only be read by clicking on a link titled "Ransomware" which leads direct to a file helpfully named "Ransomware.pdf".

In case you've been living under a rock, large chunks of the digitised world, including most of the NHS, were, ahem, *digitally disrupted* by the WannaCrypt ransomware last week.

"Following the ransomware cyber attack on Friday 12 May which affected the NHS and is believed to have affected other organisations globally, the City of London Police's National Fraud Intelligence Bureau has issued an alert urging both individuals and businesses to follow protection advice immediately and in the coming days," it said. Standard stuff.

This followed:



Please see attached.

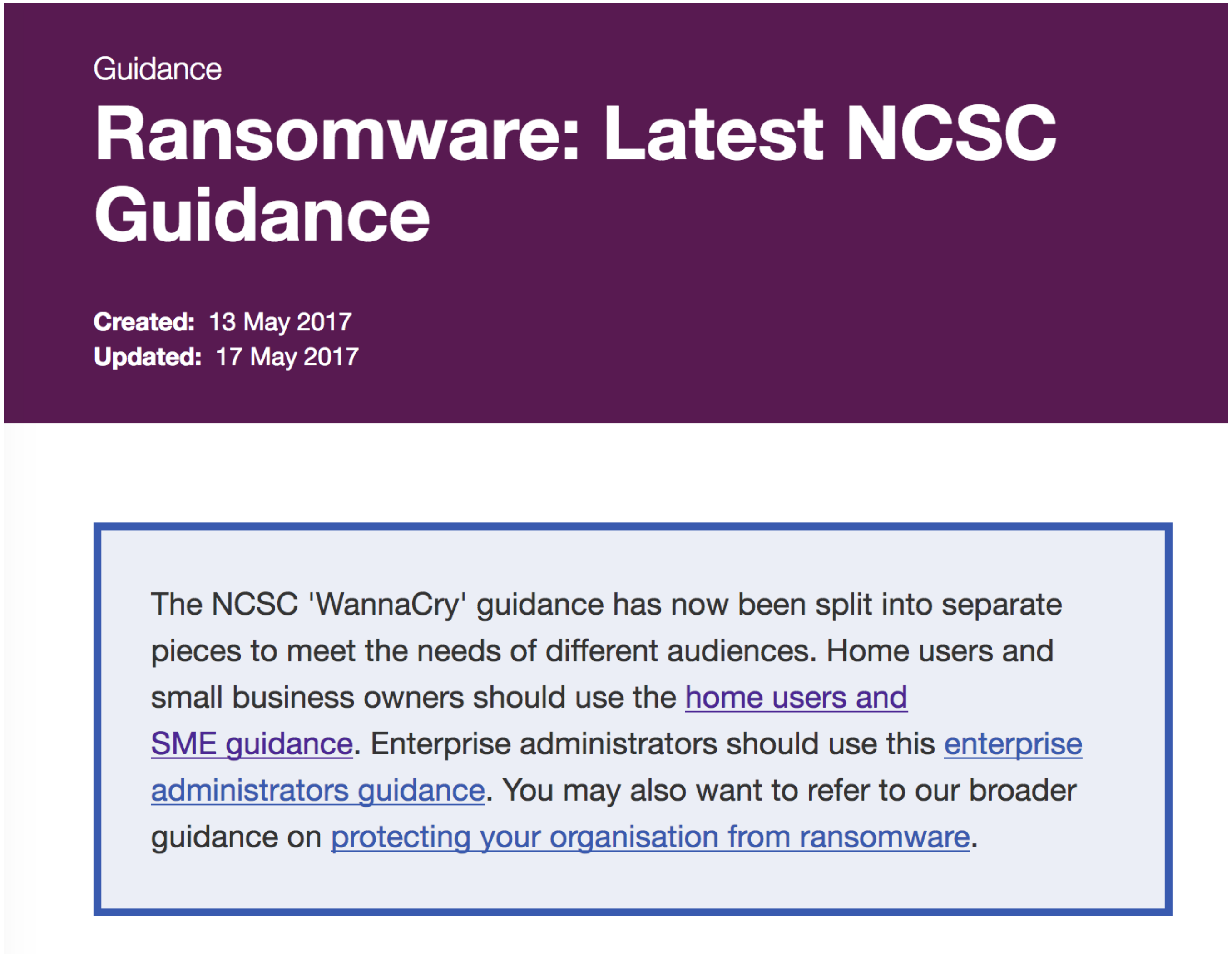
Download Associated Documents
Documents accompanying this message are linked below. Click to download and open a file which use the popular PDF format. If you experience problems downloading or viewing a file please visit this help page.

- Ransomware (423 KB)

If you need to reply regarding this message, click on this email address: [redacted]@met.pnn.police.uk

As you can see, we clicked the link – and after routing through some standard email marketing click tracker stuff, it hotlinks to a file titled "Ransomware.pdf". We chose not to let it open in our VM.

Users value trustworthy, authoritative security advice



Guidance

Ransomware: Latest NCSC Guidance

Created: 13 May 2017
Updated: 17 May 2017

The NCSC 'WannaCry' guidance has now been split into separate pieces to meet the needs of different audiences. Home users and small business owners should use the home users and SME guidance. Enterprise administrators should use this enterprise administrators guidance. You may also want to refer to our broader guidance on protecting your organisation from ransomware.

Conclusions

1. Security design must understand user activities and values, and support them
2. Paternalism is unhelpful even when it is benign – and often used to mask incompetence, vested interests, unwillingness to change
3. Users are more than willing to engage with designers who will listen, rather than flood them with geekspeak

Questions?