Security Usability: An Overview

Daniel Bosk

Department of Information and Communication Systems,
Mid Sweden University, SE-851 70 Sundsvall.

24th April 2017

Humans are incapable of securely storing high-quality cryptographic keys, and they have unacceptable speed and accuracy when performing cryptographic operations. (They are also large, expensive to maintain, difficult to manage, and they pollute the environment. It is astonishing that these devices continue to be manufactured and deployed. But they are sufficiently pervasive that we must design our protocols around their limitations.)

Kaufmann, Perlman and Speciner

What's social engineering?

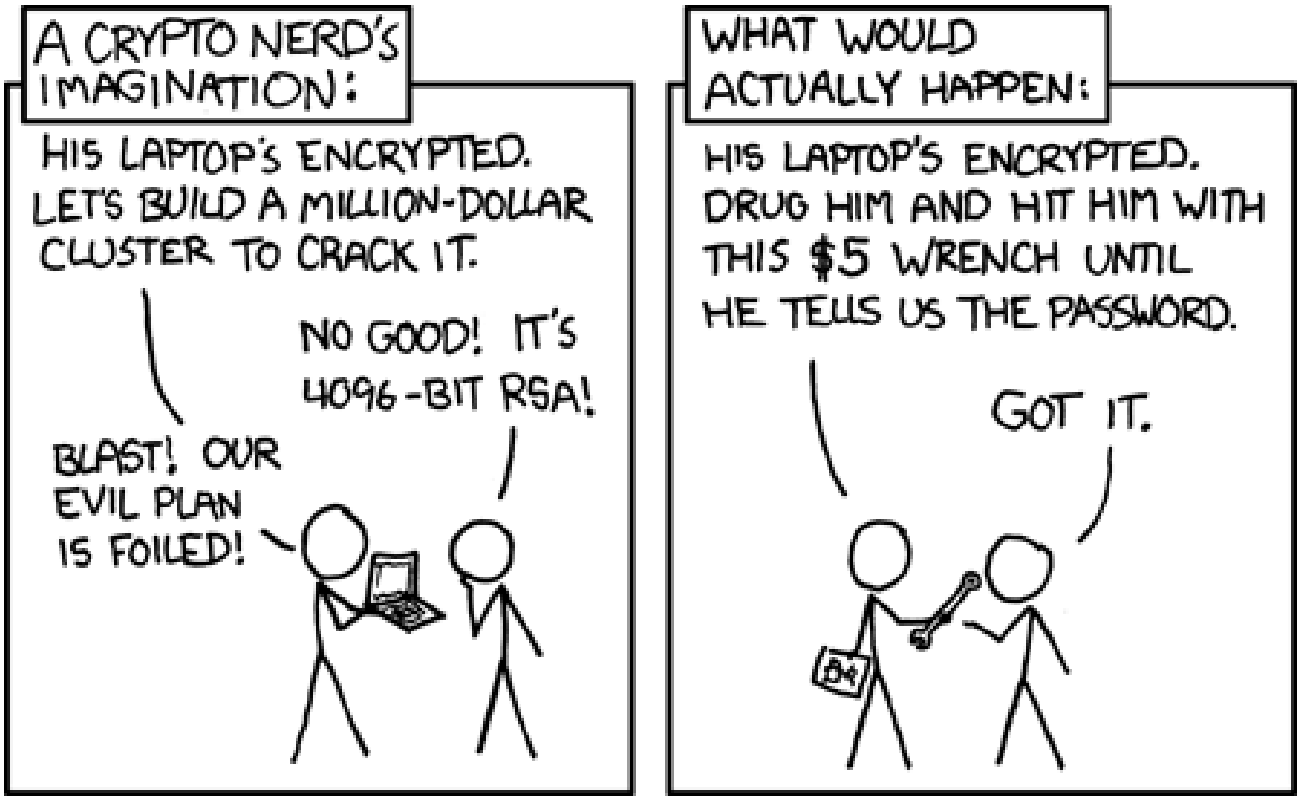

Figure: "Only amateurs attack machines; professionals target people." (Bruce Schnier). Bild: [xkcc].

What's social engineering?

- We figure out the weaknesses in human psychology.
- Then we exploit these to our advantage.

Vårt naturligt utvecklade skydd

- Vårt naturliga skydd som utvecklats under miljontals år är baserat på 'här och nu'.
- Hotet har bytt kontext under de senaste decennierna.
- Evolutionen är betydligt långsammare . . .

Definition (Pretexting)

- Att ringa någon som har tillgång till informationen och låtsas vara behörig att få veta.
- Exempelvis att låtsas vara behandlande läkare av en patient i en akut situation för att få ut information ur journalen.

Example

- Undersökning genomfördes i UK 1996 [And08].
- Utbildade personalen vid vårdinrättning om pretextingattacker.
- Upptäckte 30 falska samtal i veckan.

Example

- Från verkligheten [And08]: Ett falskt pressmeddelande publicerades som sade att VD avgått och att vinsten skulle räknas om.
  - Aktien föll med över 60 % innan det uppdagades.
- Generellt går denna typ attack under *social engineering*.

Example

- Vid granskning av IRS 2007 ringdes 102 personer spridda över hela organisationen upp.
- De ombads uppge sitt användarnamn och ändra sitt lösenord till ett givet värde.
- 62 av dem följde instruktionen.

Example

Användare säljer sina lösenord för en chokladkaka [TT10].

Example

- Personer tar främmande USB-minnen och använder dem med sina datorer.
  - Närmare bestämt 46 % av ekonomicheferna vid 500 börsnoterade företag [**pickupusb**].
  - 66 % innehåller sabotageprogram [Duc11].

- Militära organisationer har alltid haft varandras personal som måltavla för denna typer av attacker.
- De har fördelen att kunna utbilda sin personal.
- Vanliga organisationer kan också utbilda sin personal.
- Det blir desto svårare att utbilda kunder eller andra personer som berör verksamheten men inte är en del av organisationen.
- Så detta måste lösas i gränssnittet.

- Det är inte längre organisationen som angrips utan kunder och personer runt omkring.
- Angripare återanvänder riktiga e-brev med utbytta URL:er.
- Vill ha ut användarnamn, lösenord, personuppgifter, . . .

Råd

- Klicka aldrig på URL:er som skickats till dig.
- Skicka aldrig klickbara ‘Klicka här’-URL:er till någon.

Example (Mat Honan [Hon12])

- Angripare tog över och tog bort Googlekonto.
- Tog över Twitterkonto och postade kränkande kommentarer.
- Tog över AppleID-konto och tog bort alla data från alla Apple-enheter.

Example (Hur? [Hon12])

- Brister hos Amazon.
- Brister hos AppleCare.
- Olycklig koppling av e-postadresser för Me.com och Gmail.
- Detta gav dem även Twitter.

Mental models

- Mentala modeller låter oss identifiera människor, ljud, 'koncept' bättre än datorer.
- Dock gör oss även sårbara när fel modell aktiveras eller modellen inte är i linje med verkligheten.

Example (Säker anslutning)

- Användaren förstår inte SSL/TLS.
- Hänglåset betyder säkerhet.
- En phishingsida har ett signerat certifikat.

Mental models

- Mentala modeller låter oss identifiera människor, ljud, 'koncept' bättre än datorer.
- Dock gör oss även sårbara när fel modell aktiveras eller modellen inte är i linje med verkligheten.

Example (Säker anslutning)

- Användaren förstår inte SSL/TLS.
- Hänglåset betyder säkerhet.
- En phishingsida har ett signerat certifikat.

Capture errors

Ett inövat beteende används istället för korrekt.

Example

- Svänger ut på motorvägen mot Sundsvall istället för Härnösand.
- Åker hem istället för till affären efter jobbet.
- Klickar 'automatiskt' på OK-knappen utan att tänka efter.

Capture errors

Ett inövat beteende används istället för korrekt.

Example

- Svänger ut på motorvägen mot Sundsvall istället för Härnösand.
- Åker hem istället för till affären efter jobbet.
- Klickar ‘automatiskt’ på OK-knappen utan att tänka efter.

Post-completion error

När målet är nått är uppgiften genomförd, eller . . .

Example

- Uttagsautomater som ger pengarna före kortet gör att fler glömmer kortet i automaten.

Post-completion error

När målet är nått är uppgiften genomförd, eller . . .

Example

- Uttagsautomater som ger pengarna före kortet gör att fler glömmer kortet i automaten.

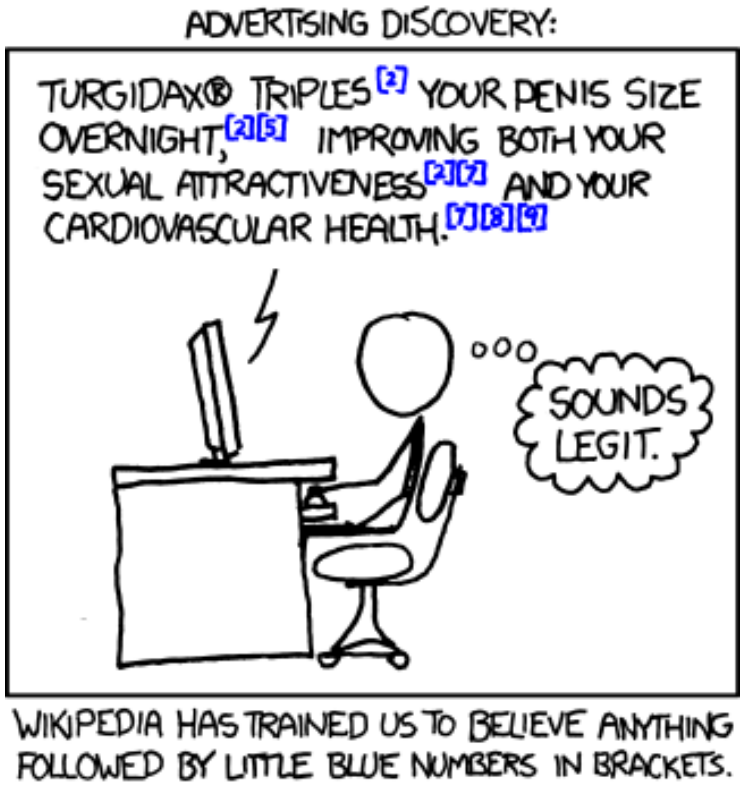

Figure: En kort seriestrip om hur vi är okritiska mot text som, till synes, har referenser. Bild: [xkca].

Cognitive load

- Kognitiv belastning påverkar oss hårt.
- Handlingar som följer någon form av regel.
- Vid hög kognitiv belastning kan fel regel följas, exempelvis starkaste regeln istället för lämpligaste.

Example

- Det är säkert då det står ‘https’ i URL:en, eller ikonen med hänglåset.
- Att hitta bankens namn är en starkare regel än att tänka på dess position;
  `https://www.swedbank.se.fraudulentbanks.com`.

Cognitive load

- Kognitiv belastning påverkar oss hårt.
- Handlingar som följer någon form av regel.
- Vid hög kognitiv belastning kan fel regel följas, exempelvis starkaste regeln istället för lämpligaste.

Example

- Det är säkert då det står ‘https’ i URL:en, eller ikonen med hänglåset.
- Att hitta bankens namn är en starkare regel än att tänka på dess position;
  `https://www.swedbank.se.fraudulentbanks.com`.

Automation bias

We trust the computer to have done the work properly, so we relax.

Example

- Två studier visar att tilliten till resultaten från Google är stor.
- Studenter valde länkar högre upp i träfflistan trots att sammanfattningarna var mindre relevanta än träffar längre ned [Pan+].
- I en nyligare genomförd studie [ER13] visas att sökresultat kan förändra personers röstningspreferenser utan att uppmärksammas.
- Detta gör sökmotoroptimering till ett farligt område.

Confirmation bias

We seek out information that confirms our beliefs.

Example

- This makes us bad at testing hypotheses.
- Test if the site is a phishing site by giving it username and password.
- If the site knows them, it must be legit.

Reverse-authorization fallacy

Give me the username and password and I'll verify them.

Confirmation bias

We seek out information that confirms our beliefs.

Example

- This makes us bad at testing hypotheses.
- Test if the site is a phishing site by giving it username and password.
- If the site knows them, it must be legit.

Reverse-authorization fallacy

Give me the username and password and I'll verify them.

Confirmation bias

We seek out information that confirms our beliefs.

Example

- This makes us bad at testing hypotheses.
- Test if the site is a phishing site by giving it username and password.
- If the site knows them, it must be legit.

Reverse-authorization fallacy

Give me the username and password and I'll verify them.

Disconfirmation bias

We rather accept plausible but wrong, than implausible but correct.

Example

- If the website behaves as the bank . . .
- Then it must be the bank . . .
- Although it's run from Russia.

Disconfirmation bias

We rather accept plausible but wrong, than implausible but correct.

Example

- If the website behaves as the bank ...
- Then it must be the bank ...
- Although it's run from Russia.

Projection bias

Everyone thinks like me.

Example

- Someone designs a system and expects the users to think like the designer.
- If you're logged in, then you must be a good guy like me.

Blind-spot bias

Biases are unconscious, that makes them difficult to see for conscious thought.

- Det sociala samspelet har stor inverkan på individen.
- 1951 visades att en individ kunde bortse från uppenbara bevis bara för att följa gruppen.
- Vidare har visats att individer kan göra helt moralvidriga saker under order från en auktoritet, Officer Scott 1995–2005:
  - Ringde upp restaurangchefer och låtsades vara polis.
  - Tvingade fram strippsökningar av oskyldiga unga anställda.
- Detta kan ske även utan order från en auktoritet, Stanford Prisoner Experiment 1971:
  - 12 vakter, 12 fångar.
  - Vakterna blev snabbt sadistiska auktoriteter.

- Det sociala samspelet har stor inverkan på individen.
- 1951 visades att en individ kunde bortse från uppenbara bevis bara för att följa gruppen.
- Vidare har visats att individer kan göra helt moralvidriga saker under order från en auktoritet, Officer Scott 1995–2005:
  - Ringde upp restaurangchefer och låtsades vara polis.
  - Tvingade fram strippsökningar av oskyldiga unga anställda.
- Detta kan ske även utan order från en auktoritet, Stanford Prisoner Experiment 1971:
  - 12 vakter, 12 fångar.
  - Vakterna blev snabbt sadistiska auktoriteter.

- Det sociala samspelet har stor inverkan på individen.
- 1951 visades att en individ kunde bortse från uppenbara bevis bara för att följa gruppen.
- Vidare har visats att individer kan göra helt moralvidriga saker under order från en auktoritet, Officer Scott 1995–2005:
  - Ringde upp restaurangchefer och låtsades vara polis.
  - Tvingade fram strippsökningar av oskyldiga unga anställda.
- Detta kan ske även utan order från en auktoritet, Stanford Prisoner Experiment 1971:
  - 12 vakter, 12 fångar.
  - Vakterna blev snabbt sadistiska auktoriteter.

- Sociala medier?
- Det ser ut som att ‘alla andra’ har gjort det.
- Exempelvis bedrägerier som sprids via Facebook.
- Oftast är de orsakade av sabotageprogram.

- Sociala medier?
- Det ser ut som att ‘alla andra’ har gjort det.
- Exempelvis bedrägerier som sprids via Facebook.
- Oftast är de orsakade av sabotageprogram.

Användbarhet?

- Svårt att komma ihåg detaljer som används sällan.
- Svårt att komma ihåg detaljer som ändras ofta.
- Svårt att komma ihåg och särskilja många liknande detaljer.
- Svårt att minnas ord utan betydelse.
- Kan ej glömma på begäran.
- Att minnas är svårare än att känna igen.

- Enklare att komma ihåg saker som används ofta.
- Enklare att minnas saker i kontext.
- Men . . .

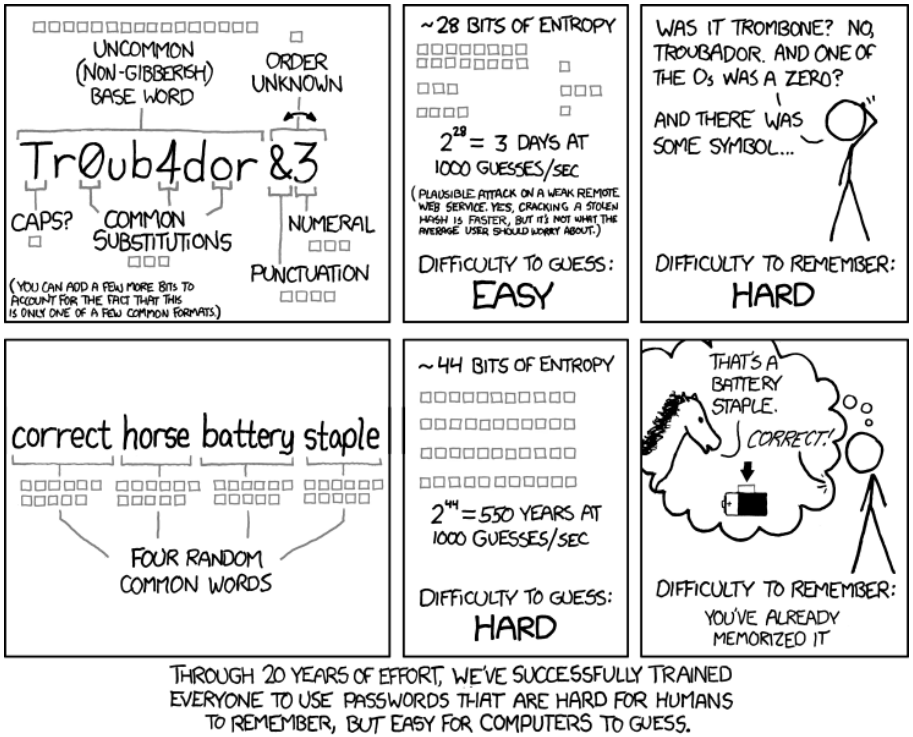

Figure: Hard to remember, easy to guess. Easy to remember, hard to guess. Bild: [xkcb].

Simson Garfinkel:

- Something you had once
- Something you've forgotten
- Something you once were.

Really?

Vet Lösenord.

Har Koddosa, som oftast skyddas av ett lösenord.

Är Fingeravtryck, som oftast kombineras med ett lösenord.

Komplexiteten hos lösenord

- PIN-koden för betalkortet, har endast tre försök sedan slutar kortet att fungera.
- Lösenordet för webbmailen, vore väldigt jobbigt om den blev låst. Hur låsa upp?
- Krypterat data, har ej kontroll över antal försök.

Komplexiteten hos lösenord

- PIN-koden för betalkortet, har endast tre försök sedan slutar kortet att fungera.
- Lösenordet för webbmailen, vore väldigt jobbigt om den blev låst. Hur låsa upp?
- Krypterat data, har ej kontroll över antal försök.

Komplexiteten hos lösenord

- PIN-koden för betalkortet, har endast tre försök sedan slutar kortet att fungera.
- Lösenordet för webbmailen, vore väldigt jobbigt om den blev låst. Hur låsa upp?
- Krypterat data, har ej kontroll över antal försök.

Example (Other types of passwords)

- Personnummer (även användarnamn).
- Kortnummer, medlemsnummer.
- Husdjurets namn.
- 'Mother's maiden name'.

Figure: En seriestrip som antyder det bisarra med säkerhetsfrågor. Namnge dina husdjur med omsorg, du kommer att använda deras namn som säkerhetsfråga resten av livet.

1. Kommer användaren att mata in rätt lösenord tillräckligt ofta?
2. Kan användaren minnas lösenordet, eller kommer denne att skriva ner det på en lapp? Väljer användaren ett lösenord som är lätt att gissa?

Example (Entering passwords)

- Muntligen ange ett nummer: hotel-, biljettbokningar, hämta ut paket från Posten.
- Mata in långa sifferkombinationer: mjukvarulicenser, refillkort, OCR-nummer för räkningar.
- Att skriva dem i grupper om tre till fyra underlättar avsevärt.
- Längre lösenord, större sannolikhet att skriva fel.

Example (Remembering passwords)

- Välj ett lösenord du inte kan minnas och skriv inte ner det.
- xkcd:s ‘correct horse battery staple’, enkelt att komma ihåg men svårare att skriva.
- Men om man bara behöver skriva det sällan, då är det mindre problem.

- Komanduri et al. [Kom+11] gjorde en undersökning om säkerhet och användbarhet hos olika lösenordspolicyer.
- Hade följande olika policyer:

  basic8 Minst åtta tecken.

  dictionary8 Minst åtta tecken, får inte finns med i ordlistan.

  comprehensive8 Minst åtta tecken, måste innehålla små och stora bokstäver, samt siffror och specialtecken.

  basic16 Minst 16 tecken.
- Säkerheten var bäst hos basic16 (högst entropi), comprehensive8 var näst bäst.
- Användbarhetsmässigt var basic16 bäst: användarna hade färre problem att skriva in lösenordet och att komma ihåg det.

- Komanduri et al. [Kom+11] gjorde en undersökning om säkerhet och användbarhet hos olika lösenordspolicyer.
- Hade följande olika policyer:

  basic8 Minst åtta tecken.

  dictionary8 Minst åtta tecken, får inte finns med i ordlistan.

  comprehensive8 Minst åtta tecken, måste innehålla små och stora bokstäver, samt siffror och specialtecken.

  basic16 Minst 16 tecken.
- Säkerheten var bäst hos basic16 (högst entropi), comprehensive8 var näst bäst.
- Användbarhetsmässigt var basic16 bäst: användarna hade färre problem att skriva in lösenordet och att komma ihåg det.

- Komanduri et al. [Kom+11] gjorde en undersökning om säkerhet och användbarhet hos olika lösenordspolicyer.
- Hade följande olika policyer:

basic8	Minst åtta tecken.
dictionary8	Minst åtta tecken, får inte finns med i ordlistan.
comprehensive8	Minst åtta tecken, måste innehålla små och stora bokstäver, samt siffror och specialtecken.
basic16	Minst 16 tecken.

- Säkerheten var bäst hos basic16 (högst entropi), comprehensive8 var näst bäst.
- Användbarhetsmässigt var basic16 bäst: användarna hade färre problem att skriva in lösenordet och att komma ihåg det.

Example (Real passwords)

Från [Obe10]:

- 123456
- password
- 12345678
- qwerty
- abc123

Från [Clu12]:

- 123456
- password
- welcome
- ninja
- abc123

Trusted path

Vi måste veta om vi kan lita på kommunikationskanalen.

Example

- Är det ett riktigt tangentbord, eller är det utbytt mot ett som sparar alla tangenttryckningar?
- Finns risken att det är en keylogger installerad?

Trusted path

Vi måste veta om vi kan lita på kommunikationskanalen.

Example

- Är det ett riktigt tangentbord, eller är det utbytt mot ett som sparar alla tangenttryckningar?
- Finns risken att det är en keylogger installerad?

- Lösenord är har i sig dålig användbarhet.
- Finns olika metoder för att förbättra användbarheten.
  - Single sign-on, exempelvis via Google eller Facebook.
  - Spara alla lösenord krypterat och fyll automatiskt i dem på webben. (Sabba inte detta alternativ med JavaScript.)
  - Komplettera med koddosa.
- Då har vi reducerat N lösenord till endast ett lösenord att komma ihåg.
- BankID verkar också vara en robust lösning.

- Lösenord är har i sig dålig användbarhet.
- Finns olika metoder för att förbättra användbarheten.
  - Single sign-on, exempelvis via Google eller Facebook.
  - Spara alla lösenord krypterat och fyll automatiskt i dem på webben. (Sabba inte detta alternativ med JavaScript.)
  - Komplettera med koddosa.
- Då har vi reducerat N lösenord till endast ett lösenord att komma ihåg.
- BankID verkar också vara en robust lösning.

BankID

- Innebär att vi måste ha någonting: certifikatet.
- Vi måste veta någonting: lösenordet för certifikatet.

BankID hos Swedbank

Inloggning

I identify myself at:
Swedbank och Sparbankerna

Godkänna (signera) överföring

I sign at:
Swedbank och Sparbankerna

Text to be signed:
Jag godkänner överföring med totalsumman 60,00 kr. Uppdraget lämnar jag till banken 2013-04-14 kl 21:25:43.

BankID hos Skatteverket

Inloggning

I identify myself at:
Skatteverket

Signering av deklaration

I sign at:
Skatteverket

Text to be signed:
Härmed undertecknar jag uppgifterna jag tidigare lämnat in.

BankID

- Har separata mekanismer för identifiering och signering.
- Kan alltså inte lura användaren att signera en överföring vid inloggning.
- Har ett användbart och pålitligt användargränssnitt.

- Utforma autentisering för att användaren inte enkelt ska kunna bli lurad!
- Om användaren blir lurad en gång ska inte det vara hela världen.

Bättre lösningar?

- Yubikey?
- LastPass?

- Träna användare att använda säkra lösenord.
- Gör det *enkelt* att använda säkra lösenord.
- Värdera lösenordet lika starkt som det som skyddas.
- Ge negativ återkoppling på dåliga lösenord.
- Men begär inte något de inte klarar av, då kommer policyn aldrig följas.

- Marknadsföringsavdelningen vill skicka länkar.
- Var konsistent, ge inte användaren delade budskap.
- Låt dem inte göra det om ni försöker att träna användarna att använda bokmärken eller skriva URL:en.
- Outsourceade kundundersökningar: från er (?), men med konstiga URL:er: ‘There’s something phishy going on.’

[And08] Ross J. Anderson. *Security Engineering. A guide to building dependable distributed systems*. 2nd ed. Indianapolis, IN: Wiley, 2008. ISBN: 978-0-470-06852-6 (hbk.) URL: http://www.cl.cam.ac.uk/~rja14/book.html.

[Clu12] Graham Cluley. *The worst passwords you could ever choose exposed by Yahoo Voices hack*. July 2012. URL: http://nakedsecurity.sophos.com/2012/07/13/yahoo-voices-poor-passwords/.

[Duc11] Paul Ducklin. *Lost USB keys have 66% chance of malware*. Dec. 2011. URL: http://nakedsecurity.sophos.com/2011/12/07/lost-usb-keys-have-66-percent-chance-of-malware.

[ER13] Robert Epstein and Ronald E. Robertson. *Democracy at risk: Manipulating search rankings can shift voting preferences substatially without voter awareness*. Tech. rep. American Institute for Behavioural Research and Technology, 2013. URL: http://aibrt.org/downloads/EPSTEIN_and_Robertson_2013-Democracy_at_Risk-APS-summary-5-13.pdf.

[Hon12] Mat Honan. 'How Apple and Amazon Security Flaws Led to My Epic Hacking'. In: *WIRED* (Aug. 2012). URL: https://www.wired.com/2012/08/apple-amazon-mat-honan-hacking/ (visited on 13/03/2017).

[Kom+11] Saranga Komanduri, Richard Shay, Patrick Gage Kelley, Michelle L. Mazurek, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor and Serge Egelman. 'Of passwords and people: Measuring the effect of password-composition policies'. In: *CHI*. 2011. URL: http://cups.cs.cmu.edu/rshay/pubs/passwords_and_people2011.pdf.

[Obe10] Jon Oberheide. *Brief analysis of the Gawker password dump*. Dec. 2010. URL: https://duo.com/blog/brief-analysis-of-the-gawker-password-dump/.

[Pan+] B. Pan, H. Hembrooke, T. Joachims, L. Lorigo, G. Gay and L. Granka. 'In Google we trust: Users' decisions on rank, position, and relevance'. In: *Journal of Computer-Mediated Communication* 12.3 (). URL: http://jcmc.indiana.edu/vol12/issue3/pan.html.

[TT10] TT. 'Folk byter lösenord mot choklad'. In: *Dagens Nyheter* (19th Jan. 2010).

[xkca] xkcd. *Adertising Discovery*. URL: https://xkcd.com/906/.

[xkcb] xkcd. *Password Strength*. URL: https://xkcd.com/936/.

[xkcc] xkcd. *Security*. URL: https://xkcd.com/538/.