CyTRAP Labs

Roentgenstrasse 49 Street

CH-8005 Zuerich Zip Code

Switzerland Country

+41(0)44 272 1876 Voice

+41(0)76 200 7778 Cell

www.CyTRAP.eu/ URL

CyTRAP Labs

Why information security awareness initiatives have failed and will continue to do so

> Back to the future – risky choices and Windows

Urs E. Gattiker
CyTRAP Labs GmbH

CyTRAP Labs

What is the message for today?

>11 – 26 years of age – risky choices

>strategies aimed at making adolescents

wiser,
less impulsive, or
less shortsighted.

are not and will continue not to be very successful in changing behaviors and risk-taking

CyTRAP Labs

_Empower user – defining a concept

How does empowerment work?

CyTRAP Labs

_Empower user – defining a concept
How does empowerment work?

power what is it?

power to install equipment?
knowledge to understand
windows?
awareness about security & cybercrime issues
taking the risks that one should take?

sociological, psychological, economic and organizational dimension

More at http://blog.cytrap.eu/?p=282

CyTRAP Labs

_Prevention

user education & awareness initiatives

CyTRAP Labs

_Prevention
user education & awareness initiatives

Is it that hard to think twice?

before clicking on an e-mail attachment that could be infected by malware

Do users not know about the consequences of an outbreak?

Migros (largest CH-retailer) March 2005, 2000 PCs infected by Rbot worm making them inoperable and, therefore having to send staff home for two days

More at Worms and Going Home While Being Paid
http://casescontact.org/euist_view.php?newsID=3609

_Prevention
user education and awareness initiatives

C'mon, it's not that hard

corporate users are sometimes even less careful, as it's not their machine and if it's broken, it's not their problem ➔ since the IT department will fix it

ENISA study on information security awareness initiatives 2007

http://blog.cytrap.eu/?p=262

➔ most security awareness initiatives do not address the effect of such factors as: gender, age, knowledge level of users, operating system used, software used, etc.

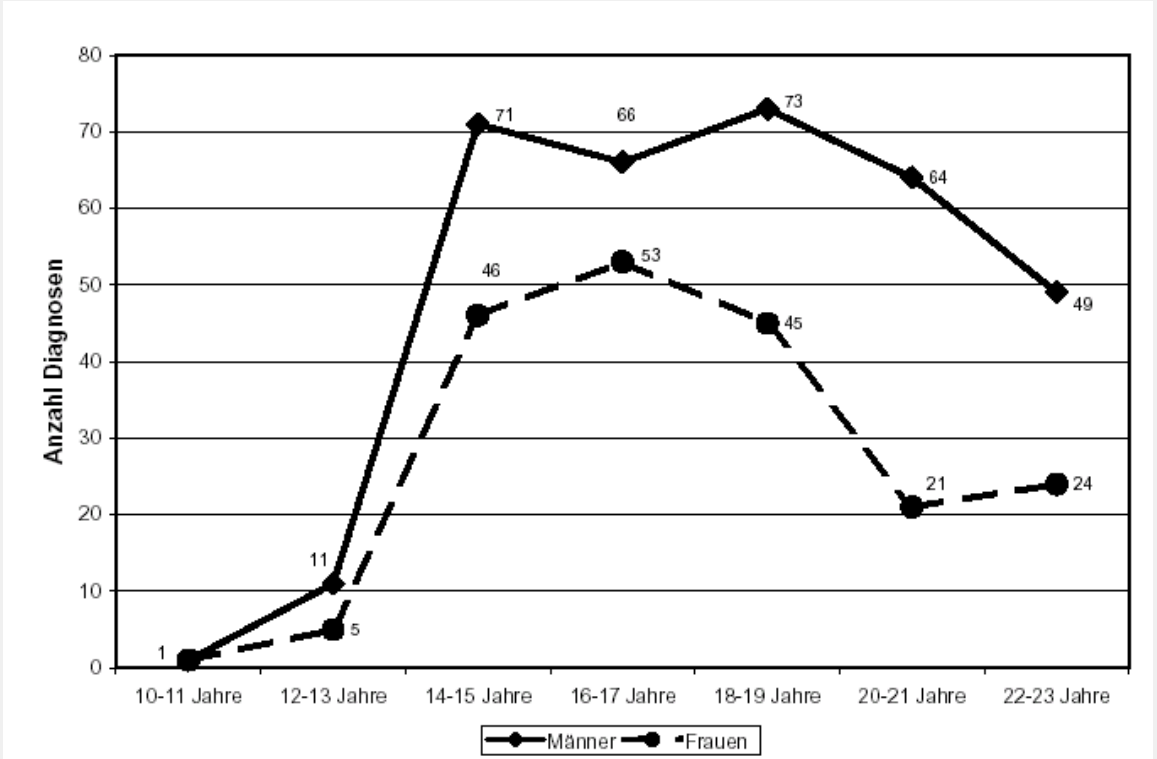
_Adolescence

_Adolescence - binge drinking – hospital data – 2003 - Switzerland

>goes up until 14-15
>cases start dropping around 19 years of age

>statistics show limiting accessibility helps reduce binge drinking (e.g., stores do not sell alcohol after 19:00 hours to anybody)

>political will to change this pattern?



Source from

http://www.sfa-ispa.ch/index.php?IDtheme=64&IDarticle=1346&IDcat24visible=1&langue=D
http://www.sfa-ispa.ch/index.php?IDtheme=26&IDarticle=1345&IDcat7visible=1&langue=F

CyTRAP Labs

_Adolescence driving when intoxicated – alcohol – 2006 – Switzerland – Mo - Fri

>goes up until 14-15
>cases start dropping around 19 years of age

>statistics show limiting accessibility helps reduce binge drinking (e.g., stores do not sell alcohol after 19:00 hours to anybody)

>political will is still lacking

Alter	Verletzte			Getötete	Case fatality ∅ 2002–2006	Getötete und Schwerverletzte pro 100 000 Einwohner
	leicht	schwer	Total			
			Werktag (Mo–Fr)			
0–6	7	0	7	0	294	0.0
7–14	17	0	17	0	0	0.0
15–17	54	19	73	1	125	7.5
18–24	243	69	312	5	250	12.0
25–44	470	161	631	12	251	7.8
45–64	261	113	374	9	362	6.2
65–74	46	17	63	3	492	3.2
75+	11	7	18	2	940	1.6
Total	**1 109**	**386**	**1 495**	**32**	**288**	**5.6**

Source from
http://www.bfu.ch/English/STATSPdfs/2006/06_18e.pdf

CyTRAP Labs

_Adolescence Driving when intoxicated – alcohol – 2006 – Switzerland – Sat - Sun

>goes up until 14-15
>cases start dropping around 19 years of age

>statistics show weekends are bad indeed – deaths

>should we go on talking or do more spot checks?

Alter	Verletzte leicht	Verletzte schwer	Total	Getötete	Case fatality ∅ 2002–2006	Getötete und Schwerverletzte pro 100 000 Einwohner
			Wochenende (Sa–So)			
0–6	10	0	10	0	238	0.0
7–14	19	6	25	0	97	0.9
15–17	65	26	91	1	136	10.1
18–24	357	111	468	10	307	19.6
25–44	396	136	532	10	292	6.6
45–64	147	64	211	5	378	3.5
65–74	22	5	27	0	185	0.8
75+	10	3	13	0	690	0.5
Total	**1 026**	**351**	**1 377**	**26**	**297**	**5.1**

Source from
http://www.bfu.ch/English/STATSPdfs/2006/06_18e.pdf

CyTRAP Labs

_Risk

CyTRAP Labs

_Risk

user education and awareness initiatives

Don't users know enough about risks?

binge drinking
driving while being intoxicated

visiting a strange website
divulging information about oneself on social networks
not having one's PC become part of a botnet that distributes spam and child pornography

What are the chances of getting caught?
What are the consequences of getting caught?

_Risk - decision-making moderators for better protection

Adapted and expanded upon from Gattiker, U. E. 2007, Information Systems Control Journal http://regustand.cytrap.eu/?p=65

	Event	Decisions based on Experience - Malware	Decisions based on Description - Firewall
Rare Events	Virus cannot be removed from PC	Underweighting of rare events – „it won‘t happen to me again!“ (Migros example – send people home for 2 days – having to pay them)	Overweighting of rare events – whole network has to be shut down – see Migros Firewall – disallowing outgoing traffic
It helps to provide an example or information that is easy for a PC user to relate to	Not being careful with one´s e-mail address will increase the amount of spam one receives	People should do the right thing but depends on if **cue validition** works (e.g., erratic outbound traffic – see firewall monitor)	Information is given more weight
How do users decide? To illustrate, consider a proposition such as this action could damage the PCs hard-drive – just raising the issue enhances its subjective truth	Information processing uses one-reason decision mechanisms – heuristics or fast-and-frugal reasoning as mental shortcuts	User knows which cues could be a valid indicator, this becomes **first step in making decision what to do** (e.g., malware found on hard-disk - backup all data on external drive NOW, re-format hard-disk and re-install Windows, thereafter scan and sanitize files saved on external drive for malware)	Little knowledge about the security/compliance or risk management environment may lead to a minimalist heuristic, whereby the **description is used as a starting point to check other cues before deciding** An invalid or confusing description will affect quality of decision negatively and increase time required to arrive at decision

CyTRAP Labs

_Risk

Information clouding minds will lead to poor choices

(e.g., information given to user by firewall, anti-virus software and system components)

>relative risk can be misleading

a mammography screening reduces mortality risk by 25%

b anti-virus software screening of incoming/outgoing mail reduces infection risk by 25%

>absolute risks can lead to greater understanding

a explaining that 25% mortality reduction means going from 4 cancer deaths out of 1,000 women without screening to 3 out of 1,000 with screening

b explaining that 25% infection reduction means going from 20 people having serious problems out of 100 users without anti-virus protection to 3 out of 100 having a serious problem with anti-virus protection installed and updated

CyTRAP Labs

_Conclusion

Our message

Download slides as a pdf file from:

http://info.cytrap.eu/?p=115

CyTRAP Labs

_Conclusion

Our message – risky choices are a fact

>11 – 26 years of age – risky choices

>awareness raising or training alone will not do

>strategies aimed at making adolescents

wiser,
less impulsive, or
less shortsighted

are not and will continue not to be very successful in changing behaviors and risk-taking regarding driving, health and cybercrime

_Conclusion

Our message – the rich get richer

> users and awareness raising – empowerment

> more competent users express more interest in additional training
these users are more likely to attend a volundary training session about IT security and operating one's PC more safely than others

> users with low competence are often unaware of their lack of skills
hence, they are not motivated to participate in training programs to increase awareness about information security

CyTRAP Labs

_Conclusion

Our message - communicate properly

> What can one do about it

Disaster strikes – how to get better protection for next time – risky choices

http://blog.CASEScontact.org (cure Windows = Wincurity)

http://mobility.CyTRAP.eu (German - telework)

CyTRAP Labs tip	(10-30 minutes to make it happen)
CyTRAP Labs quicktip	(5-10 minutes to surf safer)

_Conclusion

Our message – tell user about absolute risk

> Absolute risk means we get upset about situations like:

1: 10 chance having to re-install Windows within the next 12 months

1: 5 chance Windows must be re-installed due to malware

> Appealing to the person´s self-interest such as 1:5 will suffer from:

wasting time, loosing work, getting into trouble with regulators because of having to:

- re-install software (e.g., Windows operating system)
- loosing files with the last two days of work one did
- failing to comply to government regulation regarding data archiving
- having to pay to replace equipment

_Conclusion

Our message - summary

> address moderating variables such as age, gender, knowledge levels

> one reason decision mechanisms – heuristics, is the first indicator valid (do not drink and drive ➔ have one drink max at the GovCert.NL reception) – for PC = waste of time, spam, etc.

> enforce the rules (road checks on weekends, who controls if my home PC is part of a botnet?)

> absolute risk – 1 : 5 chance to become an identity theft victim – tell it as it is

> be ready by offering user down-to-earth help – how to – fact is MOST users are open to advice after disaster struck

_Appendix

Where can I get more info?

CyTRAP Labs

_Appendix

Where can I get more info?

Who is behind this Early Warning System (EWS)?

CyTRAP Labs (http://info.cytrap.eu/?page_id=100)
with support/collaboration from such organizations as:

- CASES.lu (http://www.CASES.public.lu)
- EICAR (http://www.EICAR.org)
- others

CyTRAP Labs

_Appendix
Where can I get more info?

How is material made accessible to the public besides Web?

e-mail or RSS to subscribers http://CASEScontact.org/subscribe_all.php

redistributed by others, such as:
- FiRST.org newsroom, MySpace, Wikipedia, etc.
- various lists on Google, Yahoo!, etc.

media (online, print and radio) (e.g., PC-Welt, Heise Security, The Times and BBC Click Online

CyTRAP Labs

_Appendix
Where can I get more info?

What services are being offered for organizations?

CyTRAP Labs Early Warning System – EWS
http://info.cytrap.eu//?page_id=12

CyTRAP Labs outsourcing - compliance and privacy functions
http://info.cytrap.eu//?page_id=14

CyTRAP Labs StratMedia - why a first place on Google search results does not sell your product or service
http://info.cytrap.eu//?page_id=24

CyTRAP Labs

Thanks

Urs E. Gattiker
CyTRAP Labs & CASEScontact.org