

“Still Clueless . . . After All These Years.”

*How to Make Your Security
Awareness Program FAIL!*

Winn Schwartau

+1 727 393 6600

Founder, SecurityExperts.com,

Founder, TheSecurityAwarenessCompany.com

Winn@TheSecurityAwarenessCompany.Com



42%: Epic Fail



60-80%: Epic Fail



**BEFORE USING A USB STICK
WHETHER YOU FOUND IT OR BOUGHT IT
MAKE SURE TO REFORMAT IT
ON A CLEAN MACHINE**

Sometimes criminals will leave **USB sticks** "in the wild" for people to find. These are called **Road Apples**. They often contain **autorun** files which can **infect a computer** just by plugging in the device. Make sure you are aware of company policy regarding bringing in USB sticks and other data devices into our *networks*.

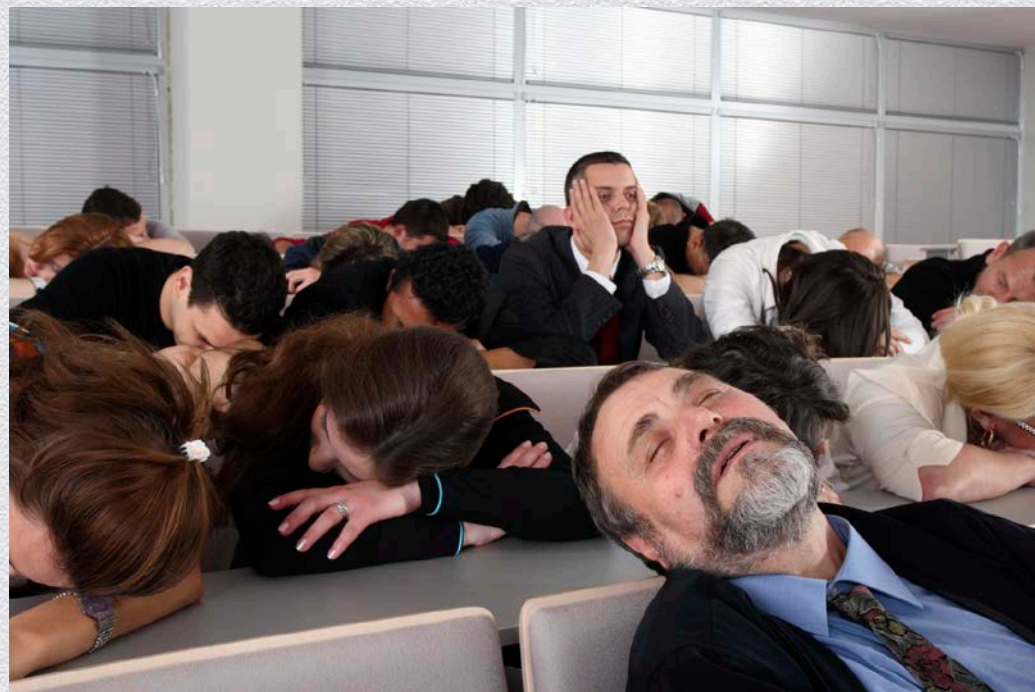
© 2012 The Security Awareness Company






Awareness Must Be Boring



the security awareness
C O M P A N Y



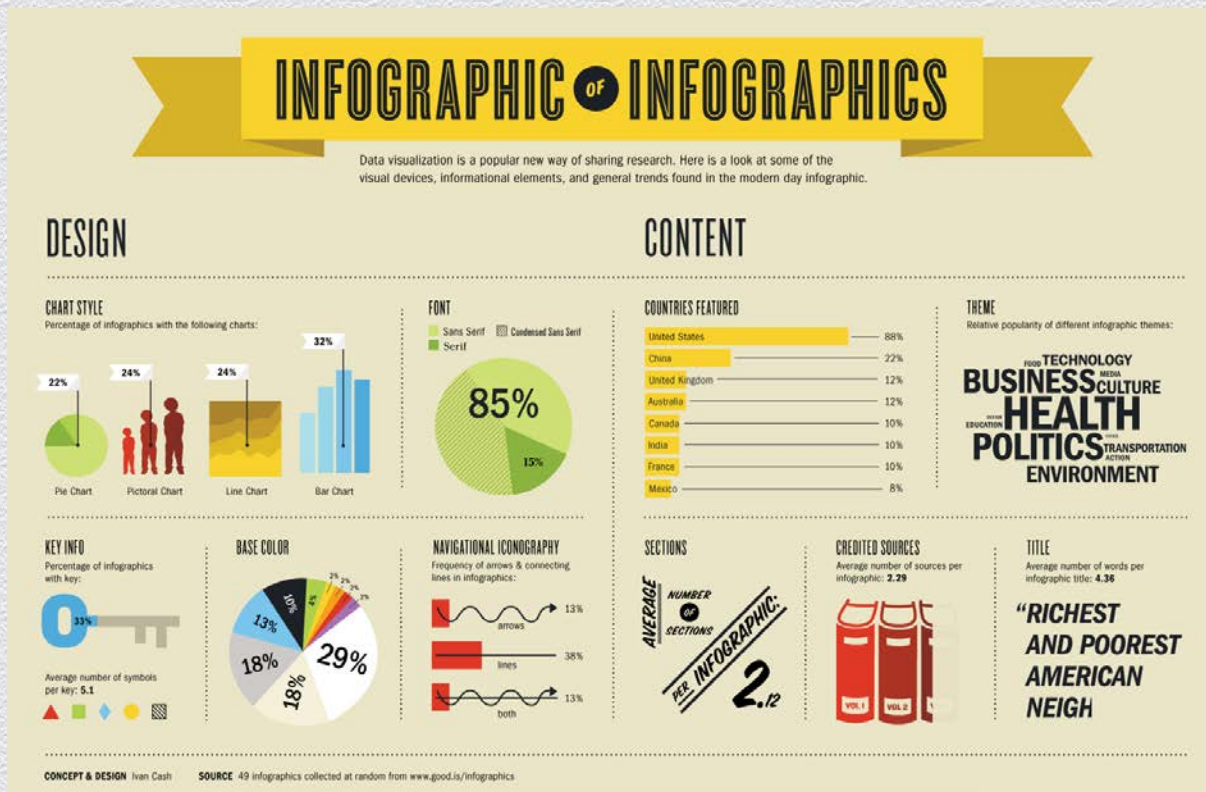
-  Mind numbingly so, if budget permits.
-  Words, words and more words.
-  Extra dull earns extra points!



Graphics Just Get in the Way



the security awareness
C O M P A N Y



Why waste time organizing information in infographics? Eight pages of agonizingly small 7.5pt font is just as effective, right?



If you **DO** break down and use graphics, don't waste time hiring graphic designers: all graphics are created equal.

Tell - Don't Show



the security awareness
C O M P A N Y



SAC

Multi-media is cheesy, silly and overrated. Videos are pointless.

SAC

Tell in lots of words. Never 'show' or create visual metaphors.

SAC

Videos do not reinforce information in a memorable way. Email instructions is just fine, thank you!



Never Use Humor



the security awareness
C O M P A N Y

- SAC** Work and security require a business attitude. If people laugh are they really paying attention?
- SAC** In fact, smiling is discouraged. People should understand the serious nature of security.





the security awareness
C O M P A N Y

All You Need to Teach Is Policy



YOU CAN'T DO THAT
YOU MUST DO THIS
NO

SAC

Repeat the same dry, boring rules over and over again. People will get it.

SAC

Knowing policy means no security breaches.





the security awareness
C O M P A N Y

Do Not Make Awareness Personal



Don't acknowledge a person's family or personal lives. Concern should only lie with the company and whether that is secure or not. Everything else is expendable.



Remember, when in doubt, just follow policy.



Confuse Awareness With Training



the security awareness
C O M P A N Y



Coke obviously wastes \$3B/Yr. on Global Brand Awareness



Repetitive multi-media branding is useless. It doesn't change behavior.



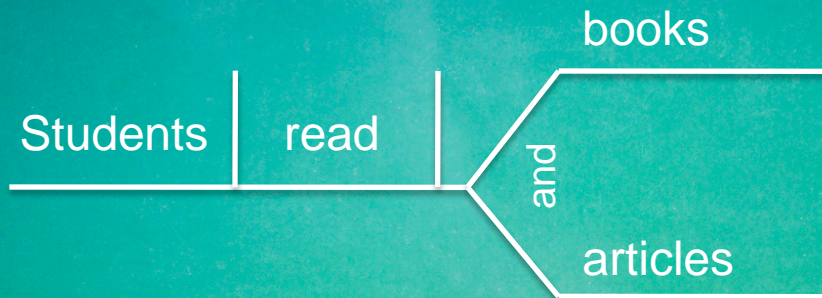
Brilliant marketing is a myth. Don't buy into the hype.



Hire An English Major & Parse



the security awareness
C O M P A N Y



Analyze communication until it's as complicated and dry as possible



In order to communicate clearly, an individual needs a Master's Degree. At least. Otherwise, communicate at your own risk.

Never Use Casual Written or Spoken Language



the security awareness
C O M P A N Y

Gonna HACKERS
Blind Eye SECURITY
AWARENESS
Flim Flam
Scam Man
SPEAK GEEK?
INS AND OUTS OF SOCIAL
ENGINEERING
DNS TCP/IP
IPS DLP TLS
SIEM AES



Casual is Unprofessional!



Use academic terms only!



People love words and acronyms
they don't understand.

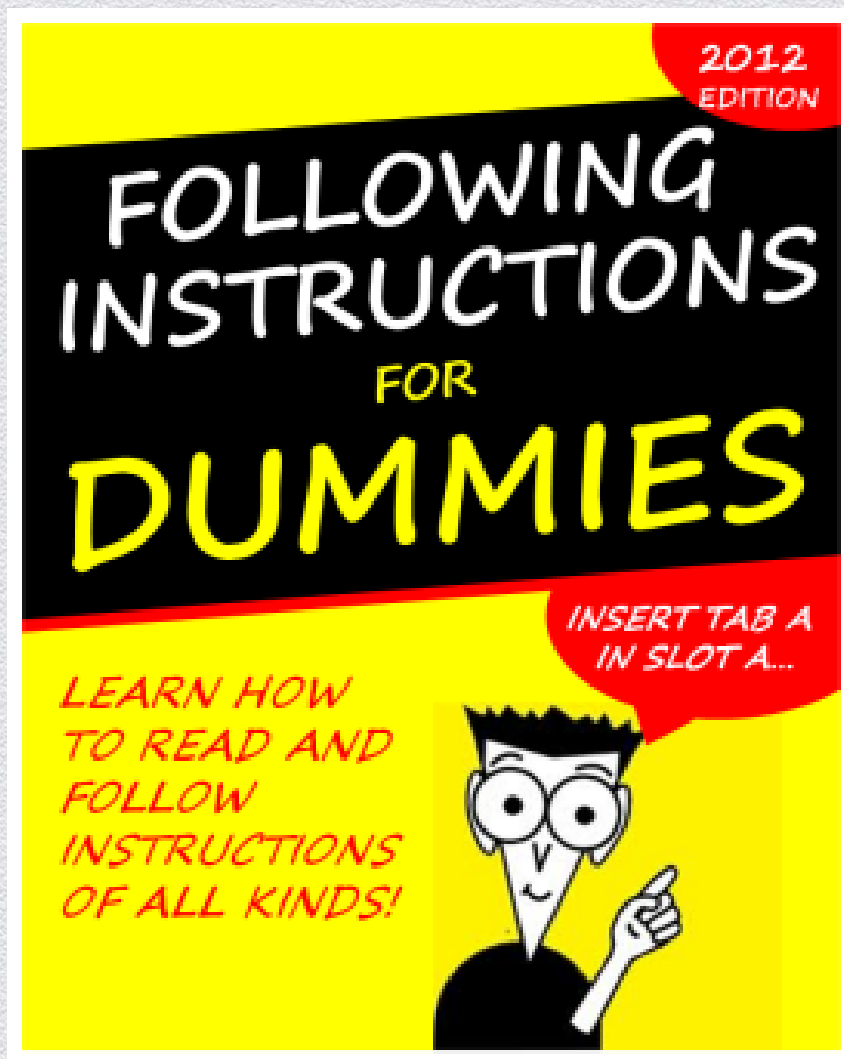
#RSAC

RSACONFERENCE2014

Do Not Violate The Formal or Structured Instructional Process



the security awareness
C O M P A N Y



Complicated instructions ensure the most secure programs



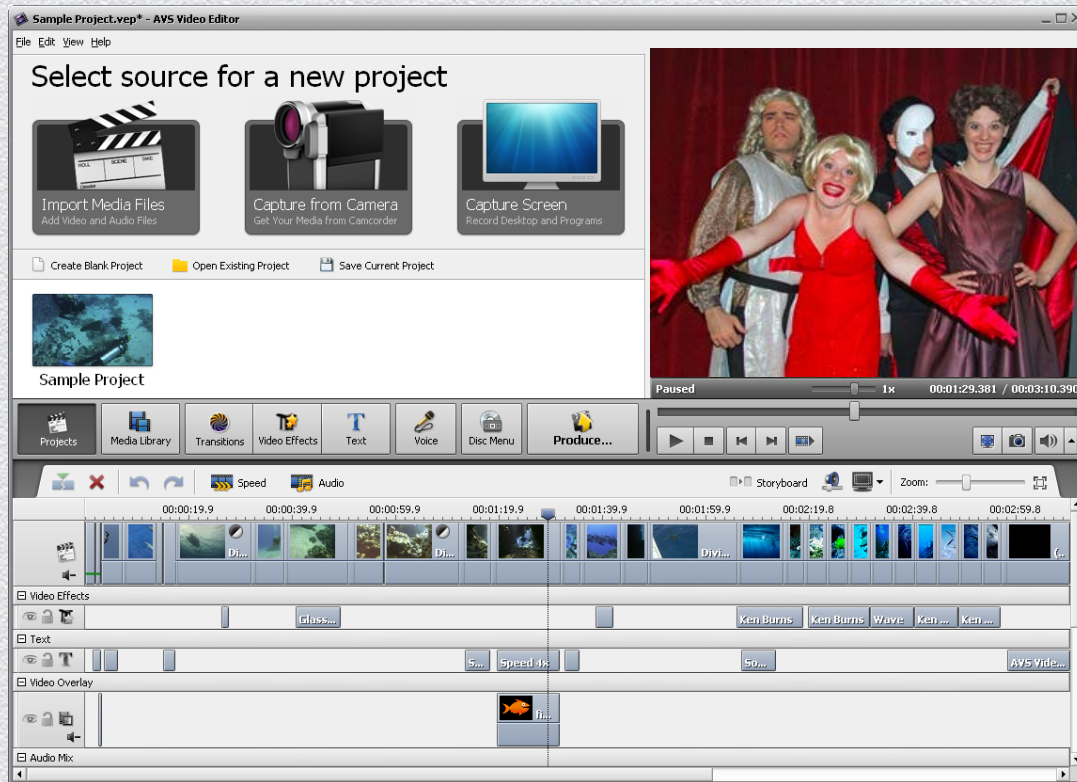
Standards should be rigid and require an instructional consultant



Let the CISO into the Production Process



the security awareness
C O M P A N Y



The CISO took a film class.



The VP-IT took a semester of creative writing.

Let them set the tone and have the final say in both graphics and editing!



the security awareness
C O M P A N Y

Let Corp Comm Run All Awareness



SAC CorpComm can build you the ‘box’ from which creative escape is impossible.

SAC Want to delay a program for months? CorpComm can help you with that.





the security awareness
C O M P A N Y

Design by Committee



SAC

Who needs leadership or technical knowledge? Add needless complexity & internal inconsistency

SAC

Who needs to waste time with a strong, creative vision? The quality of a product doesn't matter. All that matters is a committee approval.



Awareness Should Be Super Technical



the security awareness
C O M P A N Y



A helpdesk is just another mindless expense.



Who says your time is valuable? Don't go to the experts for help. Waste a couple of hours and troubleshoot the problem yourself.



#RSAC

RSACONFERENCE2014



the security awareness
C O M P A N Y

More Security Experts is Better



Make all of your employees super-geeky security experts.



Saves \$ on Tech Support.



The Execs Don't Need Security Awareness



the security awareness
C O M P A N Y



- SAC** C-Suiters don't have time to waste on security awareness.
- SAC** They approved their policies, they obviously know how to avoid security risks.
- SAC** So save your funds and don't train them.



RSACONFERENCE2014



the security awareness
C O M P A N Y

Ignore IT & Technical Staff

SAC Save money! Don't train the geeks.

SAC Geeks design the software and run the networks why would they need training?

SAC Geeks **only** have to stay up-to-date on how to manage firewalls and ensure your security. Save that extra \$100 and don't train them.



i am bored



#RSAC

RSACONFERENCE2014

Use Threats & Give Orders



the security awareness
C O M P A N Y



MOTIVATION

The firings will continue until moral improves!

DEV.DESPAIR.COM



Want to be a better leader? Use more fear.



Leadership through fear is exceedingly effective in controlling people's behavior.



#RSAC

RSACONFERENCE2014



the security awareness
C O M P A N Y


Testing Is Reliable and Accurate



SAC

Everyone who passes the test knows how to behave when a security event occurs.

SAC

Make tests super easy so everyone gets an 'A' and the auditors are happy.  #RSAC

RSACONFERENCE2014

Everyone Knows, Awareness Is Only A Once A Year Event



Once is always enough.
Especially for security.

Reinforce policy through **one** yearly video or **one** short course.

Make it mandatory and force every employee to check the “I will always follow policy” box under threat of termination; before they even take the course.



Once Is Enough



the security awareness
C O M P A N Y



SAC Have you had your once a year awareness day?

SAC Have you scored all your employees with yearly security quizzes?

SAC Checked all the right boxes?

SAC Yes! Then congrats, you're done! No need to repeat it. We're done. Right?

#RSAC

RSACONFERENCE2014

[illegible]

Comments? Questions? Responses?



Winn Schwartau, CEO

Winn@TheSecurityAwareness.Com

+1.727.393.6600



facebook.com/TheSACcompany



twitter.com/SecAwareCo



linkedin.com/company/the-security-awareness-company



The Security Awareness Company

Entertaining. Educational. Effective

Winn Schwartau, Founder & CEO

+1.727.393.6600