

# Practical Cybersecurity

Terry Zink  
Program Manager  
Microsoft



**2011**  
BARCELONA   
5-7 October 2011





# Outline

1. Introduction
2. Background
3. How to teach people
4. What we should teach them



# Background

- People fall for scams
- Our brains are programmed to fall for scams
- Education works but people are slow learners

# The problem

- Made worse because the computer industry gives bad advice!

**Top Row: 'Tr0ub4dor & 3'**

- Entropy:** ~28 bits of entropy. Calculation:  $2^{28} = 3 \text{ DAYS AT } 1000 \text{ GUESSES/SEC}$ . Note: (PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)
- Difficulty to Guess:** EASY
- Difficulty to Remember:** HARD

**Bottom Row: 'correct horse battery staple'**

- Entropy:** ~44 bits of entropy. Calculation:  $2^{44} = 550 \text{ YEARS AT } 1000 \text{ GUESSES/SEC}$
- Difficulty to Guess:** HARD
- Difficulty to Remember:** YOU'VE ALREADY MEMORIZED IT

THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.



# How can we teach users better?

- Help!
- How do professional educators do it?
- *Transfer*: the ability to take what you have learned and *transfer* it to a new situation
  - Users don't know how to *transfer* real life to cyber life
- How can we improve *transfer*?



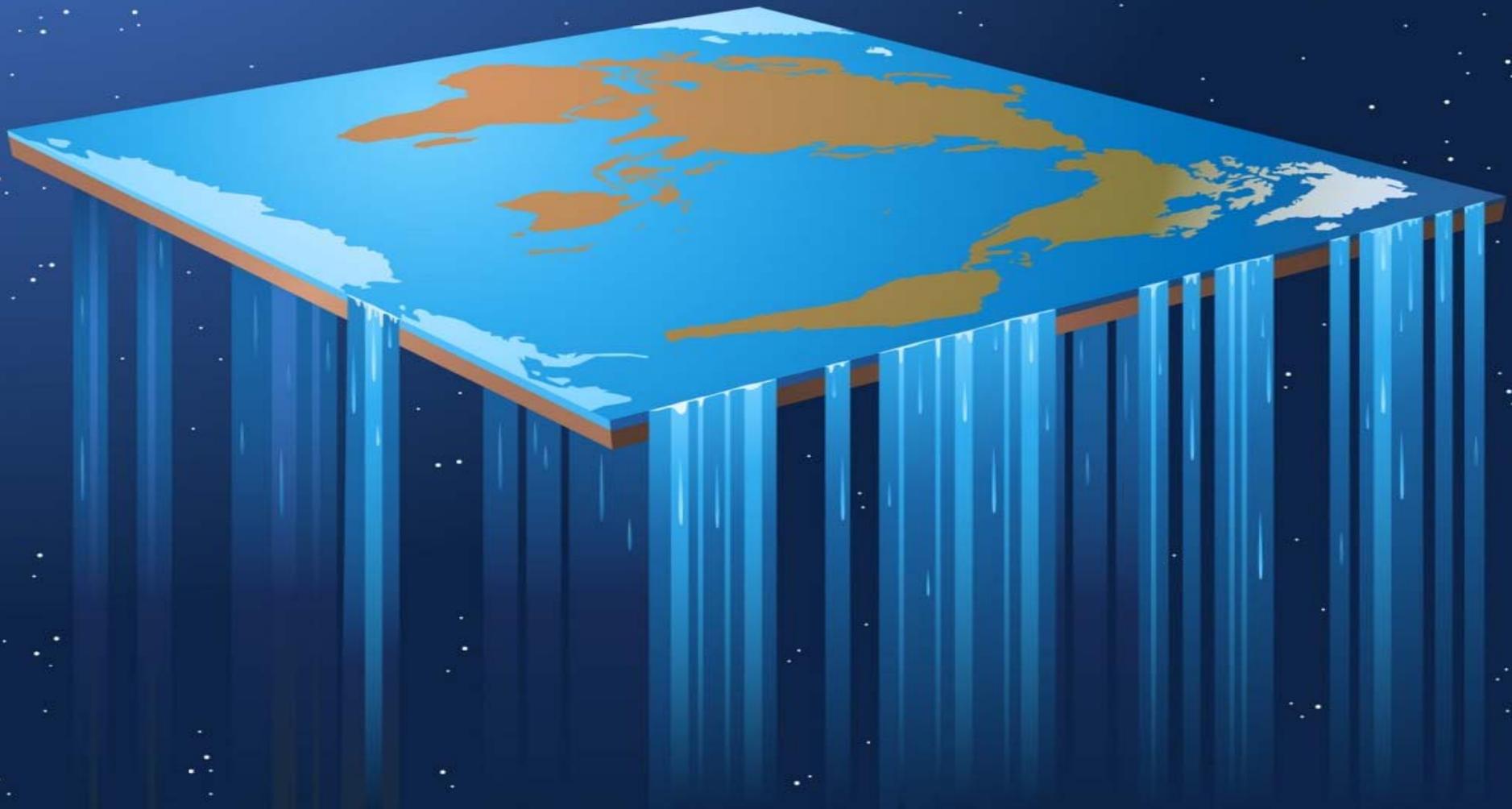


# Expertise

- People need to recognize scams
- How? Through **deliberate practice**
- Look at the aspects of the scam
- Abstract → specific
  - Be cautious → Hover mouse over a link

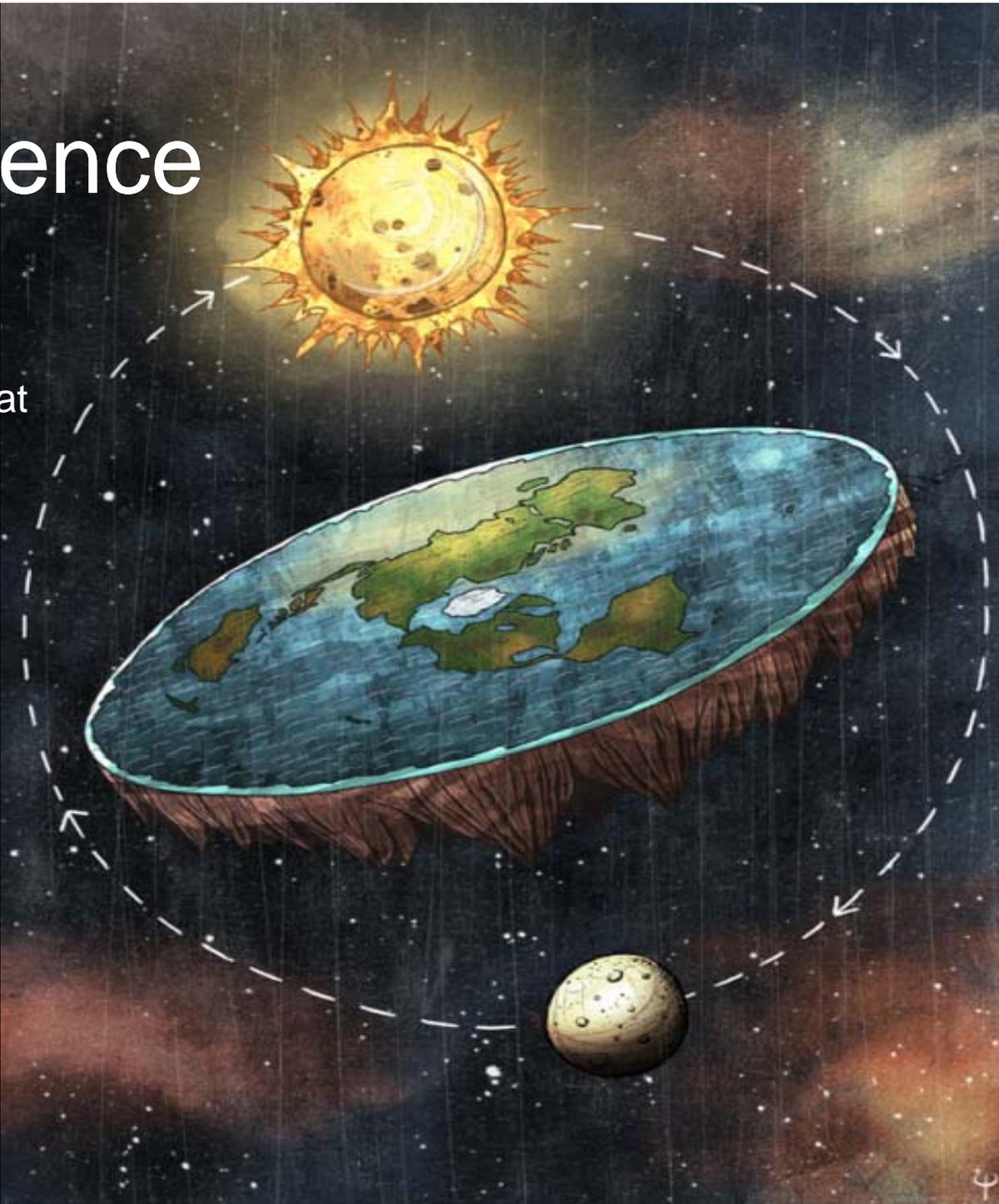
# Experience

What if you believed the earth is flat?



# Experience

But were told that  
it is round?





# Experience

- If prior beliefs are not engaged, people revert back to old models (ball of yarn)
- Fake A/V
  - People need A/V
  - Security industry is trustworthy
- Integrate new information with prior knowledge
  - People need A/V
  - **And** they need to get it from a trustworthy source
  - Abstract better than specific

# Metacognition

- “Thinking about thinking”
- The Revolutionary War
  - Why did the rebels want to secede?
  - Why did the loyalists want to remain?



# Metacognition

- *Why* won't banks ask for your password?
- Game – Think from the other side

HERO



vs

VILLAIN





# What to teach?

- The Internet is fun but only deal with trustworthy sources
- Keep your software up-to-date
- Learn to recognize scams



# How young to start?

- Start early
- Current efforts not enough
- Requires public and private partnership

# What should *we* do?

- Smart defaults
- Easy-to-update



Qualys® BrowserCheck Results

- Click the status button to read specific version information and recommended actions.
- Click Fix It to resolve the security issue.

	<b>Mozilla Firefox</b> Product Version: 4.0.1	<input type="button" value="Up To Date"/>
Installed Version: 4.0.1		
	<b>Adobe Flash Player</b> Product Version: 10.2.159.1	<input type="button" value="Insecure Version"/> <input type="button" value="Fix It"/>
	<b>Java Runtime</b> Product Version: 1.6.0_23	<input type="button" value="Insecure Version"/> <input type="button" value="Fix It"/>
	<b>Adobe Shockwave Player</b> Product Version: 11.5.9	<input type="button" value="Up To Date"/>
	<b>Apple Quicktime</b> Product Version: QuickTime 7.6.9 (1680.9)	<input type="button" value="Up To Date"/>
	<b>Microsoft Silverlight</b> Product Version: 4.0.60310.0	<input type="button" value="Up To Date"/>
	<b>Microsoft Windows Media Player</b> Product Version: 12.0.7600.16667	<input type="button" value="Up To Date"/>

<https://browsercheck.qualys.com>



# Conclusions

- Students need to know a lot of stuff, and organize it well, for that stuff to become useful to real life.
- Students take new knowledge and weave it into their pre-existing knowledge. Teachers need to know their students' prior beliefs.
- Students retain knowledge when they have to think about why they are learning something.
- Defaults matter!



# QUESTIONS?

Contact: [tzink@microsoft.com](mailto:tzink@microsoft.com)