Getting The Message Across
Explaining Security to non-Security People.

David Buerckner July 2018

"Expertise has no value to an audience that doesn't understand"

- https://www.presentation-guru.com/the-best-way-to-explain-complex-concepts-part-1/

Why is the sky blue?

https://www.youtube.com/watch?time_continue=76&v=4pnk50rhDfs

Agenda

- Your biggest risk
- Align the message to the audience
- Make the message stick

- **Keep it simple**

Why Does Getting The Message Across Matter?

Anthem—Used social engineering to gain privileged access
American health insurance company Anthem revealed in early-2015 that ...ned the personal information including names, social security ...sses, and income data of both consumers and employees. The ... attack came when one of Anthem's system administrators ...ne had used his unique identifier code to initiate a database ...w believe the attackers responsible for the breach used social ...chniques to steal the administrator's credentials and gain ...surance company's network.

eBay—Phishing attack stole credentials
In the late-spring of 2014, news first broke about a breach against the e-commerce website. An investigation later determined that a group of attackers leveraged phishing attacks to steal the credentials of as many as 100 eBay employees. They used that information to gain access to eBay's internal network, where they then exfiltrated the names, passwords, email addresses, physical addresses, and other personal information of 145 million customers. The attackers allegedly had unfettered access to eBay's systems for 229 days.

...kers sent many of Sony's top executives fake Apple ID verification emails. Each email led to a phishing site that stole a target's Apple... that someone had reused their Apple ID information... the hackers abused those usernames and passwords... employees' LinkedIn profiles to guess their way onto... gaining access, the hackers used Wiper malware to c... computer networks and make off with 100 terabytes... the United States believes were working for North Ko... much of that information online.

JPMorgan Chase—Exploited lack of two-step verification
In the spring of 2014, hackers stole the login credentials for one of the employees at JPMorgan Chase, a leading global financial services firm. Those attackers then exploited an oversight—the bank's security had forgotten to implement two-step verification (2SV) on one of the network servers—to gain access to JPMorgan Chase's corporate network. Following that initial intrusion, the attackers moved laterally across the bank's network, gaining access to 90 servers in total. They didn't steal any sensitive financial information before they were detected and blocked in August, but they did succeed in making off with the names, addresses, phone numbers, email addresses, and other information of around 76 million households and approximately 7 million small businesses.

People

- **Your** people are generally your number 1 risk

- Mandatory compliance training does not result in understanding

- The best tool you have is your ability to explain the risks **so your people understand**.

- If your people understand security risks, your life will be better.
    - Reduced risk of breaches and incidents
    - Easier to get funding or projects approved
    - Security is seen to have value

Your Target Audience (and greatest allies)

They are a prime cyber target.

They have significant influence within a business.

They hold the purse strings.

Learn how to explain IT Security to Finance people.
They can be your greatest allies.

Be Relevant To Your Audience

Before explaining how something works, make sure your audience knows what's in it for them. It is much easier to explain something to someone who wants to understand.

Vary the explanation based on the target audience.

Assume no prior knowledge, and eliminate jargon.
Make it simple.

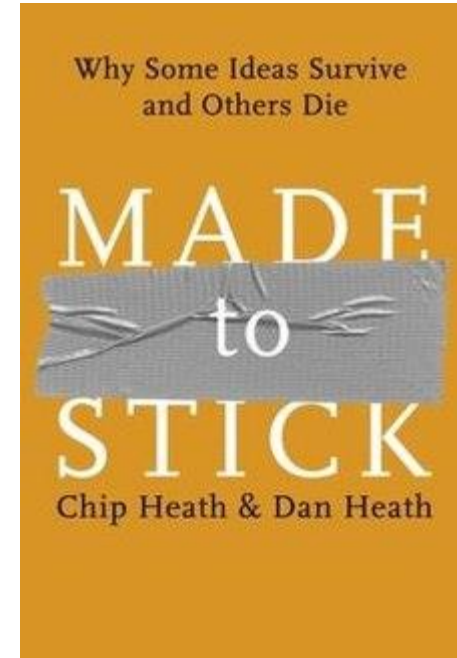Make it relatable. Use analogies but don't assume one analogy works for all.
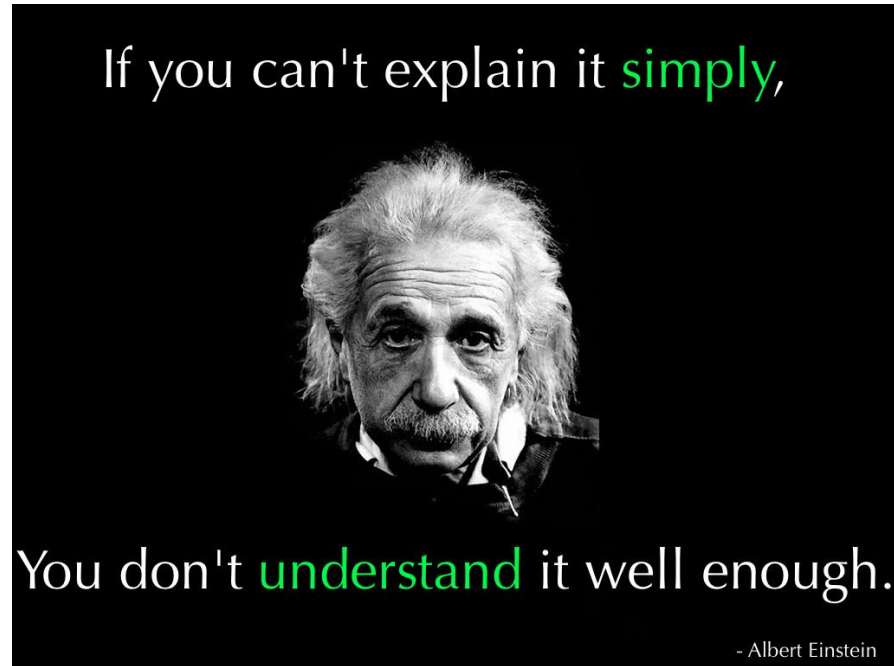
Make the explanation Stick

Make it simple.

Make it memorable.

Repeat it. Make it your signature.

Make it Simple – The Up-Goer Five Editor

http://splasho.com/upgoer5/

7. Particle physics

"Where I work, we slam together small things to break them into even smaller things until we have the smallest things possible. This is how we know what matter is made of." *Paul Sorenson, Physicist studying Quark-Gluon Plasma with the Relativistic Heavy Ion Collider at Brookhaven National Laboratory*

"There are bad people who want to make the things you see on the computer go away. Sometimes it is for money and sometimes it is a game. The simple way of making computer stuff go away is like shouting very loud so no one can hear. This makes it so you can not see the things on the computer you want until they stop shouting. I try to make them be quiet." *Christian Ternus, information security researcher*

2. Web development

"Computers are used to share pictures, words, and movies (usually of cats) with other computers. The computers need to show the cats on boxes with tiny lights in them, but don't know how. People like me tell the computer many words so that it knows how to change the tiny lights to look like a cat. We try to make the lights change very fast so that you don't have to wait for your cats. Some days the lights are all wrong, and we have to tell the computer more words to make them look like cats again."

Brandon Jones, Google Chrome GPU Team

Mothers and fathers pass their body plan to their children. These plans are written in a large number of letters, and tell each kid's body how to live. Every person has a different set of letters.

One reason why every person has a different set of letters is because sometimes, but not very often, the letters get changed to a different letter before they get into the children. Sometimes these are considered wrong letters, but sometimes they are just considered different letters. When the wrong or different letters happen, sometimes a person's body can get sick.

"Some people learn by trying things out. Some people learn by thinking very hard. I make a world inside a computer the way people think the world works, and then try things out, to see if we are thinking right."

— Computer simulation. Lots of scientists still don't understand the value of this. Matthew Hoyles.

Putting it all together – Beryl and the DDOS Attack

- Jargon?
- Simple?
- Memorable?

https://www.youtube.com/watch?v=iRd7NiFxOUA

Questions?

Call To Action

- Invest time in different ways to explain security

- Understand that your audience may have a very different type of knowledge to you

- Accept that you will benefit from as many people as possible understanding the risks associated with cyber security

- Tomorrow, take some time to create an explanation, and use it.

Contact Details

LinkedIn - https://www.linkedin.com/in/david-buerckner-4ba70010/