DefCamp #5 - Bucharest, November 28th, 2014

Social Engineering

...OR «HACKING PEOPLE»

Tudor Damian

CEH, IT solutions specialist

www.tudy.tel

https://www.youtube.com/watch?v=_G3NT91AWUE

OPERATIONS

9/3/2014
07:15 PM

Home Depot, Other Retailers Get Social Engineered

Famed annual contest reveals how many retailers lack sufficient defenses against social engineering.

Kelly Jackson Higgins
News

Connect Directly

11 COMMENTS
COMMENT NOW

In the end, it may have been a foreshadowing of sorts: The team assigned to squeeze potentially sensitive information from Home Depot employees in cold calls during this year's Social Engineering Capture the Flag (SECTF) competition at DEF CON 22 won the famed contest.

The social engineering competition held last month in Las Vegas was in no way directly related to a report yesterday that Home Depot may have suffered a massive data breach; the home improvement chain was still investigating suspicious "activity" as of this posting. However, it was among a group of major US retailers that fell to multiple social engineering tactics during the competition.

FEATURE

The human OS: Overdue for a social engineering patch

Credit: Shutterstock

MORE LIKE THIS

Security training is lacking: Here are tips on how to do it better

No money, no problem: Building a security awareness program on a shoestring...

The hacker 'skills gap' may be more of a strategy gap

InformationWeek
DARKReading
CONNECTING THE INFORMATION SECURITY COMMUNITY

PERIMETER

10/2/2014
12:07 AM

Marilyn Cohodas
Commentary

Connect Directly

Poll: Employees Clueless About Social Engineering

Not surprisingly, our latest poll confirms that threats stemming from criminals hacking humans are all too frequently ignored.

When it comes to social engineering, Pogo, the central character of a long-running American comic strip, said it best. "We have met the enemy and he is us."

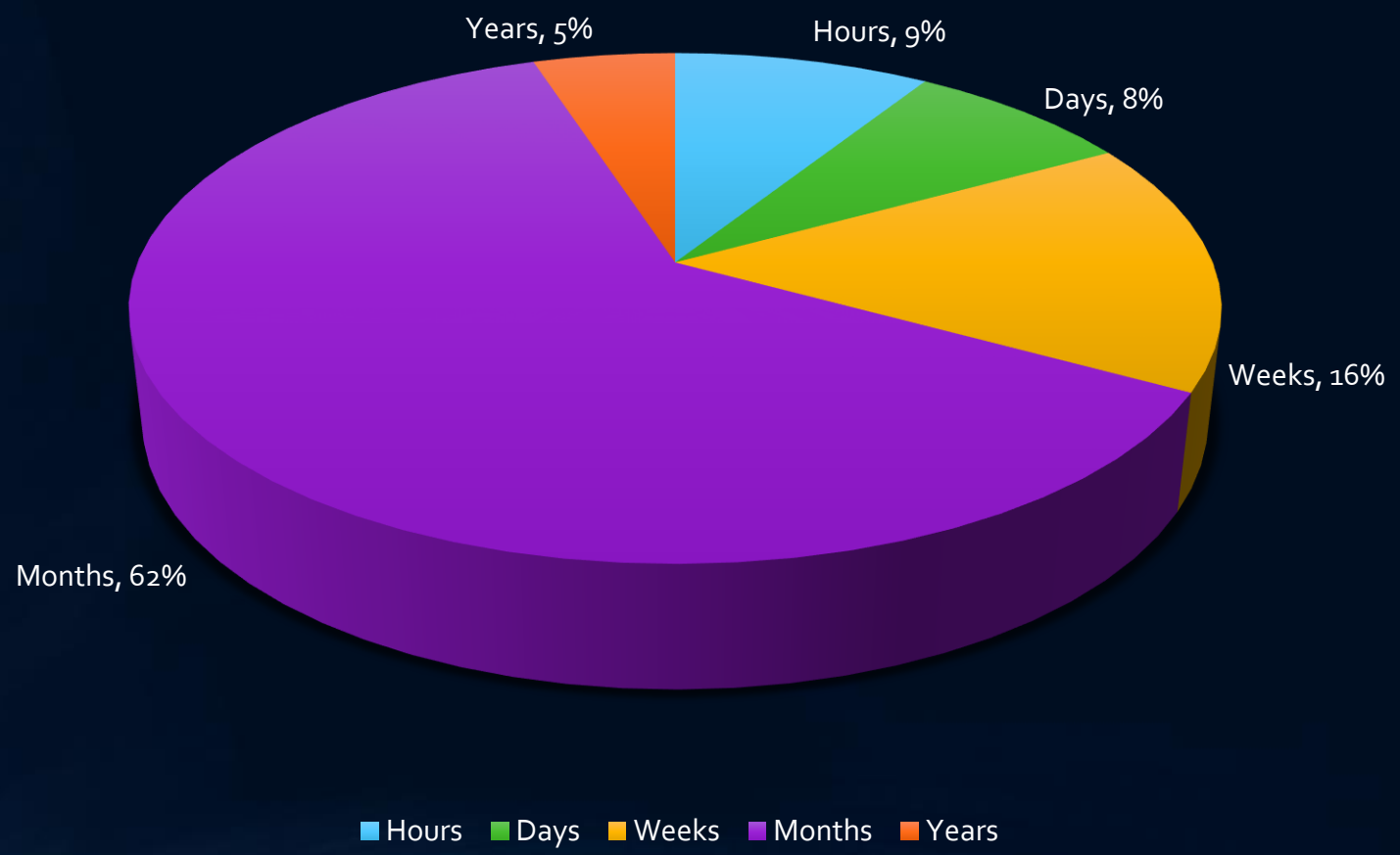
87% of small business and 93% of larger organizations experienced a cyber security breach in the last year

Source: UK Government, Department for Business, Innovation and Skills (BIS)

Did you see this: http://bit.ly/tudydefcamp ?

Most malicious attacks come from within an organization

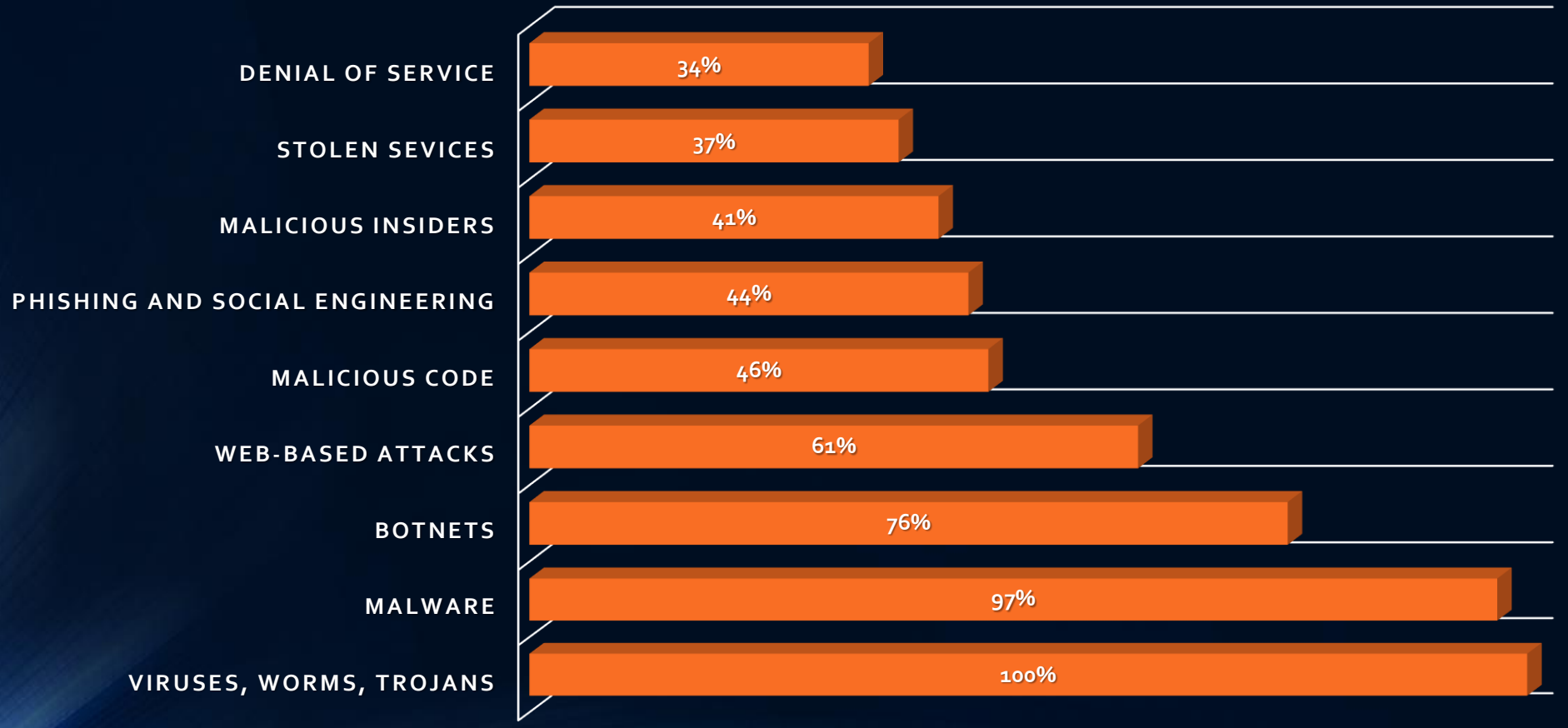
Timeline of discovery for cyber espionage attacks worldwide (2013)



Source: Verizon

Go to http://bit.ly/tudydefcamp now

Cyber crime attacks experienced by US companies (June 2014)



Source: Ponemon Institute; Hewlett-Packard (HP Enterprise Security)

So, what is Social Engineering?

Go to http://bit.ly/tudydefcamp now, ...please?

OSI Model – anything missing?

7 – Application layer

6 – Presentation layer

5 – Session layer

4 – Transport layer

3 – Network layer

2 – Link layer

1 – Physical layer

OSI Model – revised ☺

8 – Human layer

7 – Application layer

6 – Presentation layer

5 – Session layer

4 – Transport layer

3 – Network layer

2 – Link layer

1 – Physical layer

Social Engineering, or "Hacking People"

- The science of making people do what you want
- Attacks the most vulnerable layer in the OSI model ☺

Why are people vulnerable?

- False Assumptions
  - If X is true, then Y is true; Y is true, therefore X must be true
- Logical Fallacies
  - Incorrect arguments in logic and rhetoric, resulting in a lack of validity
- Cognitive Biases
  - Patterns of deviation in judgment, whereby inferences about other people and situations may be drawn in an illogical fashion
- Heuristics & Mental Shortcuts
  - Used to speed up the process of finding a satisfactory solution via mental shortcuts
    - e.g. using a rule of thumb, an educated guess, an intuitive judgment, stereotyping, profiling, common sense, etc.
  - Eases the cognitive load of making a decision

strawman

Misrepresenting someone's argument to make it easier to attack.

By exaggerating, misrepresenting, or just completely fabricating someone's argument, it's much easier to present your own position as being reasonable, but this kind of dishonesty serves to undermine rational debate.

After Will said that we should put more money into health and education, Warren responded by saying that he was surprised that Will hates our country so much that he wants to leave it defenceless by cutting military spending.

false cause

Presuming that a real or perceived relationship between things means that one is the cause of the other.

Many people confuse correlation (things happening together or in sequence) for causation (that one thing actually causes the other to happen). Sometimes correlation is coincidental, or it may be attributable to a common cause.

Pointing to a fancy chart, Roger shows how temperatures have been rising over the past few centuries, whilst at the same time the numbers of pirates have been decreasing, thus pirates cool the world and global warming is a hoax.

slippery slope

Asserting that if we allow A to happen, then Z will consequently happen too, therefore A should not happen.

The problem with this reasoning is that it avoids engaging with the issue at hand, and instead shifts attention to baseless extreme hypotheticals. The merits of the original argument are then tainted by unsubstantiated conjecture.

Colin Closet asserts that if we allow same-sex couples to marry, then the next thing we know we'll be allowing people to marry their parents, their cars and even monkeys.

ad hominem

Attacking your opponent's character or personal traits in an attempt to undermine their argument.

Ad hominem attacks can take the form of overtly attacking somebody, or casting doubt on their character. The result of an ad hom attack can be to undermine someone without actually engaging with the substance of their argument.

After Sally presents an eloquent and compelling case for a more equitable taxation system, Sam asks the audience whether we should believe anything from a woman who isn't married, was once arrested, and smells a bit weird.

special pleading

Moving the goalposts or making up exceptions when a claim is shown to be false.

Humans are funny creatures and have a foolish aversion to being wrong. Rather than appreciate the benefits of being able to change one's mind through better understanding, many will invent ways to cling to old beliefs.

Edward Johns claimed to be psychic, but when his 'abilities' were tested under proper scientific conditions, they magically disappeared. Edward explained this saying that one had to have faith in his abilities for them to work.

loaded question

Asking a question that has an assumption built into it so that it can't be answered without appearing guilty.

Loaded question fallacies are particularly effective at derailing rational debates because of their inflammatory nature - the recipient of the loaded question is compelled to defend themselves and may appear flustered or on the back foot.

Grace and Helen were both romantically interested in Brad. One day, with Brad sitting within earshot, Grace asked in an inquisitive tone whether Helen was having any problems with a fungal infection.

the gambler's fallacy

Believing that 'runs' occur to statistically independent phenomena such as roulette wheel spins.

This commonly believed fallacy can be said to have helped create a city in the desert of Nevada USA. Though the 'overall odds of a 'big sum' happening may be low, each spin of the wheel is itself entirely independent from the last.

Red had come up six times in a row on the roulette wheel, so Greg knew that it was close to certain that black would be next up. Suffering an economic form of natural selection with this thinking, he soon lost all of his savings.

bandwagon

Appealing to popularity or the fact that many people do something as an attempted form of validation.

The flaw in this argument is that the popularity of an idea has absolutely no bearing on its validity. If it did, then the Earth would have made itself flat for most of history to accommodate this popular belief.

Shamus pointed a drunken finger at Sean and asked him to explain how so many people could believe in leprechauns if they're only a silly old superstition. Sean, however, had had a few too many Guinness himself and fell off his chair.

black-or-white

Where two alternative states are presented as the only possibilities, when in fact more possibilities exist.

Also known as the false dilemma, this insidious tactic has the appearance of forming a logical argument, but under closer scrutiny it becomes evident that there are more possibilities than the either/or choice that is presented.

Whilst rallying support for his plan to fundamentally undermine citizens' rights, the Supreme Leader told the people they were either on his side, or on the side of the enemy.

begging the question

A circular argument in which the conclusion is included in the premise.

This logically incoherent argument often arises in situations where people have an assumption that is very ingrained, and therefore taken in their minds as a given. Circular reasoning is bad mostly because it's not very good.

The word of Zorbo the Great is flawless and perfect. We know this because it says so in The Great and Infallible Book of Zorbo's Best and Most Truest Things that are Definitely True and Should Not Ever Be Questioned.

appeal to authority

Saying that because an authority thinks something, it must therefore be true.

It's important to note that this fallacy should not be used to dismiss the claims of experts, or scientific consensus. Appeals to authority are not valid arguments, but nor is it reasonable to disregard the claims of experts who have a demonstrated depth of knowledge unless one has a similar level of understanding.

Not able to defend his position that evolution 'isn't true' Bob says that he knows a scientist who also questions evolution (and presumably isn't herself a primate).

composition /division

Assuming that what's true about one part of something has to be applied to all, or other, parts of it.

Often when something is true for the part it does also apply to the whole, but because this isn't always the case it can't be presumed to be true. We must show evidence for why a consistency will exist.

Daniel was a precocious child and had a liking for logic. He reasoned that atoms are invisible, and that he was made of atoms and therefore invisible too. Unfortunately, despite his thinky skills, he lost the game of hide and go seek.

appeal to nature

Making the argument that because something is 'natural' it is therefore valid, justified, inevitable, good, or ideal.

Many 'natural' things are also considered 'good,' and this can bias our thinking, but naturalness itself doesn't make something good or bad. For instance murder could be seen as very natural, but that doesn't mean it's justifiable.

The medicine man rolled into town on his bandwagon offering various natural remedies, such as very special plain water. He said that it was only natural that people should be wary of 'artificial' medicines like antibiotics.

anecdotal

Using personal experience or an isolated example instead of a valid argument, especially to dismiss statistics.

It's often much easier for people to believe someone's testimony as opposed to understanding variation across a continuum. Scientific and statistical measures are almost always more accurate than individual perceptions and experiences.

Jason said that that was all cool and everything, but his grandfather smoked, like, 30 cigarettes a day and lived until 97 - so don't believe everything you read about meta analyses of sound studies showing proven causal relationships.

appeal to emotion

Manipulating an emotional response in place of a valid or compelling argument.

Appeals to emotion include appeals to fear, envy, hatred, pity, guilt, and more. Though a valid, and reasoned, argument may sometimes have an emotional aspect, one must be careful that emotion doesn't obscure or replace reason.

Luke didn't want to eat his sheep's brains with chopped liver and brussels sprouts, but his father told him to think about the poor, starving children in a third world country who weren't fortunate enough to have any food at all.

tu quoque

Avoiding having to engage with criticism by turning it back on the accuser - answering criticism with criticism.

Literally translating as 'you too' this fallacy is commonly employed as an effective red herring because it takes the heat off the accused having to defend themselves and shifts the focus back onto the accuser themselves.

Nicole identified that Hannah had committed a logical fallacy, but instead of addressing the substance of her claim, Hannah accused Nicole of committing a fallacy earlier on in the conversation.

burden of proof

Saying that the burden of proof lies not with the person making the claim, but with someone else to disprove.

The burden of proof lies with someone who is making a claim, and is not upon anyone else to disprove. The inability, or disinclination, to disprove a claim does not make it valid (however we must always go by the best available evidence).

Bertrand declares that a teapot is, at this very moment, in orbit around the Sun between the Earth and Mars, and that because no one can prove him wrong his claim is therefore a valid one.

no true scotsman

Making what could be called an appeal to purity as a way to dismiss relevant criticisms or flaws of an argument.

This fallacy is often employed as a measure of last resort when a point has been lost. Seeing that a criticism is valid, yet not wanting to admit it, new criteria are invoked to dissociate oneself or one's argument.

Angus declares that Scotsmen do not put sugar on their porridge, to which Lachlan points out that he is a Scotsman and puts sugar on his porridge. Furious, like a true Scot, Angus yells that no **true** Scotsman sugars his porridge.

the texas sharpshooter

Cherry-picking data clusters to suit an argument, or finding a pattern to fit a presumption.

This 'false cause' fallacy is coined after a marksman shooting at barns and then painting a bullseye target around the spot where the most bullet holes appear. Clusters naturally appear by chance, and don't necessarily indicate causation.

The makers of Sugarette Candy Drinks point to research showing that of the five countries where Sugarette drinks sell the most units, three of them are in the top ten healthiest countries on Earth, therefore Sugarette drinks are healthy.

the fallacy fallacy

Presuming a claim to be necessarily wrong because a fallacy has been committed.

It is entirely possibly to make a claim that is false yet argue with logical coherency for that claim, just as is possible to make a claim that is true and justify it with various fallacies and poor arguments.

Recognising that Amanda had committed a fallacy in arguing that we should eat healthy food because a nutritionist said it was popular, Alyse said we should therefore eat bacon double cheeseburgers every day.

personal incredulity

Saying that because one finds something difficult to understand, it's therefore not true.

Subjects such as biological evolution via the process of natural selection require a good amount of understanding before one is able to properly grasp them; this fallacy is usually used in place of that understanding.

Kirk drew a picture of a fish and a human and with effusive disdain asked Richard if he really thought we were stupid enough to believe that a fish somehow turned into a human through just, like, random things happening over time.

ambiguity

Using double meanings or ambiguities of language to mislead or misrepresent the truth.

Politicians are often guilty of using ambiguity to mislead and will later point to how they were technically not outright lying if they come under scrutiny. It's a particularly tricky and premeditated fallacy to commit.

When the judge asked the defendant why he hadn't paid his parking fines, he said that he shouldn't have to pay them because the sign said 'Fine for parking here' and so he naturally presumed that it would be fine to park there.

genetic

Judging something good or bad on the basis of where it comes from, or from whom it comes.

To appeal to prejudices surrounding something's origin is another red herring fallacy. This fallacy has the same function as an ad hominem, but applies instead to perceptions surrounding something's source or context.

Accused on the 6 o'clock news of corruption and taking bribes, the senator said that we should all be very wary of the things we hear in the media, because we all know how very unreliable the media can be.

middle ground

Saying that a compromise, or middle point, between two extremes must be the truth.

Much of the time the truth does indeed lie between two extreme points, but this can bias our thinking: sometimes a thing is simply untrue and a compromise of it is also untrue. Half way between truth and a lie, is still a lie.

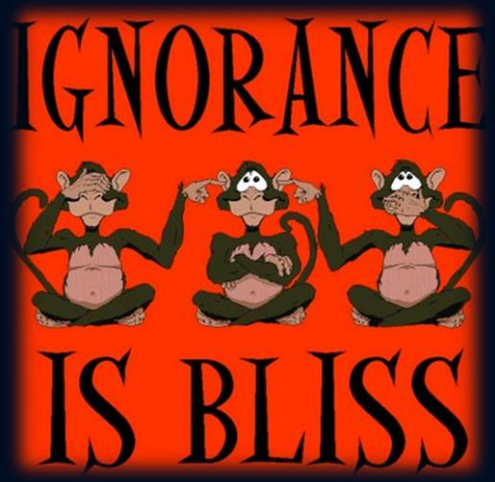
Holly said that vaccinations caused autism in children, but her scientifically well-read friend Caleb said that this claim had been debunked and proven false. Their friend Alice offered a compromise that vaccinations cause some autism.

thou shalt not commit logical fallacies

A logical fallacy is a flaw in reasoning. Strong arguments are void of logical fallacies, whilst arguments that are weak tend to use logical fallacies to appear stronger than they are. They're like tricks or illusions of thought, and they're often very sneakily used by politicians, the media, and others to fool people. Don't be fooled! This poster has been designed to help you identify and call out dodgy logic wherever it may raise its ugly, incoherent head. If you see someone committing a logical fallacy online, link them to the relevant fallacy to school them in thinkiness e.g. yourlogicalfallacyis.com/strawman

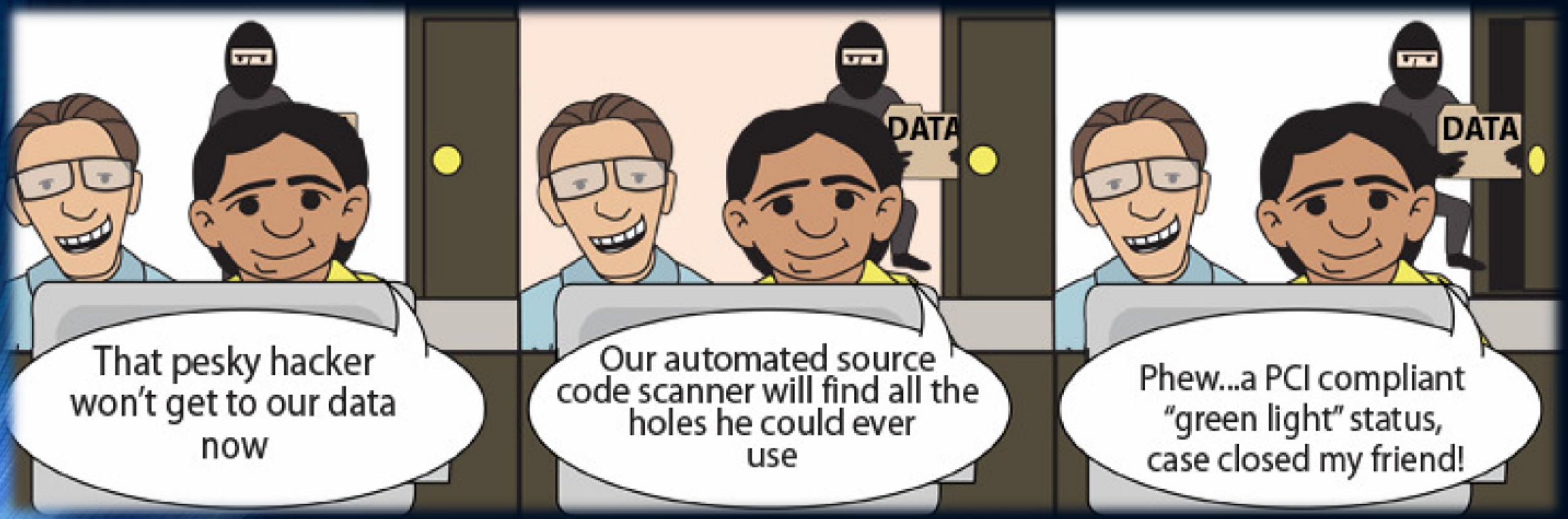
yourlogicalfallacyis.com

Behaviors vulnerable to attacks



- Human nature of trust is the basis of most SE attacks
- Ignorance about SE and its effects
- SE attackers might threaten with losses or consequences in case of non-compliance with their request
- SE attackers lure the targets to divulge information by promising something for nothing
- Targets are asked for help and they comply out of a sense of moral obligation

Technology doesn't fix ignorance



Types of Social Engineering

- Human-based Social Engineering
  - Gathers sensitive information by interaction
  - Attacks of this category exploit trust, fear and the helping nature of humans
- Computer-based or mobile-based Social Engineering
  - SE carried out with the help of computers and/or mobile apps

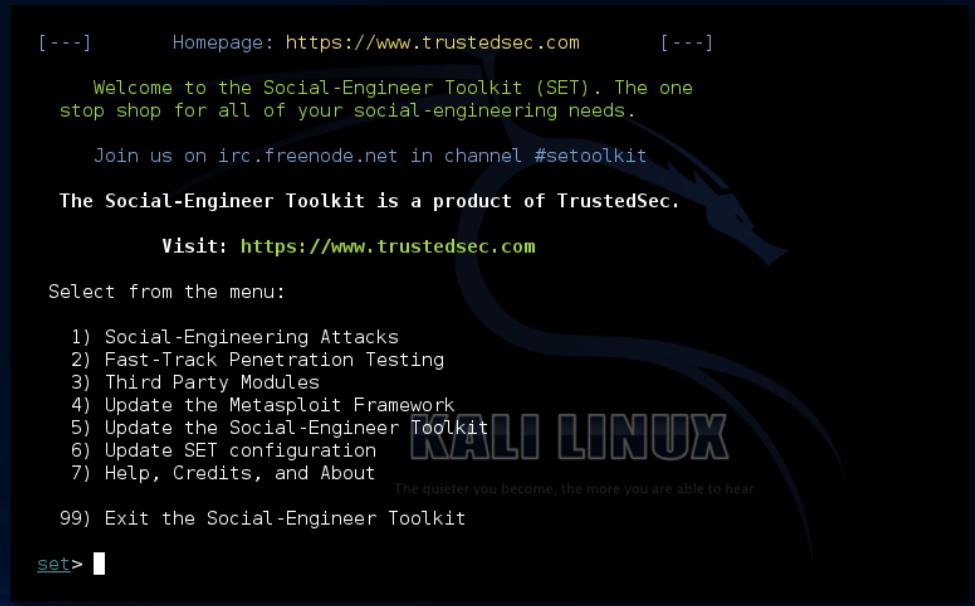
Human-based Social Engineering

- Posing as a legitimate end user
  - Give identity and ask for sensitive information
- Posing as an important user
  - Posing as a VIP of a target company, valuable customer, etc.
- Posing as technical support
  - Call as technical support staff and request credentials to retrieve data
  - Authority support
- Eavesdropping
- Shoulder surfing
- Dumpster diving
- Tailgating & Piggybacking
- Reverse SE
  - Marketing
  - Sabotage
  - Tech Support

Seriously now. http://bit.ly/tudydefcamp

Computer-based Social Engineering

- Spam Email
- Hoax/Chain Letters
- Instant Chat Messenger
- Pop-up Windows
- Phishing & Spear Phishing
- Publishing Malicious Apps
- Repackaging Legitimate Apps
- Fake Security Applications



Common Social Engineering attacks

- Email from a friend
  - May contain links/attachments with malicious software embedded
  - Messages may create a compelling story or pretext
- Phishing attempts
  - Email, IM, comment, text message appearing to come from a legitimate, popular company, bank, school, institution
  - These messages usually have a scenario or story
    - Explain there is a problem, notify you that you're a "winner", ask for help
- Baiting scenarios
- Persuasion
- Impersonation
- Response to a question you never had

Such wow, much link: http://bit.ly/tudydefcamp

Why are companies vulnerable to SE?

- Insufficient security training
- Easy Access to information
- Several Organizational Units
- Lack of security policies
- SE attacks detection is very difficult
- There's no method to ensure complete security against any form of SE attacks
- There's no specific software or hardware for defending against SE attacks

SE attack against an organization - Phases

- Research on target company
  - Dumpster diving, websites, employees, tour company, etc.
- Select victim
  - Identify the frustrated/gullible employees of the target company
- Develop relationship
  - Develop relationships with the selected employees
- Exploit the relationship
  - Collect sensitive account information, financial information and current technologies

Potential impact on the organization

- Economic losses
- Loss of privacy
- Damage of goodwill
- Temporary or permanent closure
- Lawsuits and arbitrations
  - etc.

Common targets of SE attacks

- Receptionists and Help Desk personnel
- Vendors of the target organization
- Users and clients
- Low-profile employees and staff
- Office workers
- Technical Support Executives
- System Administrators

...or a laptop? You can pull out your laptop and go to http://bit.ly/tudydefcamp

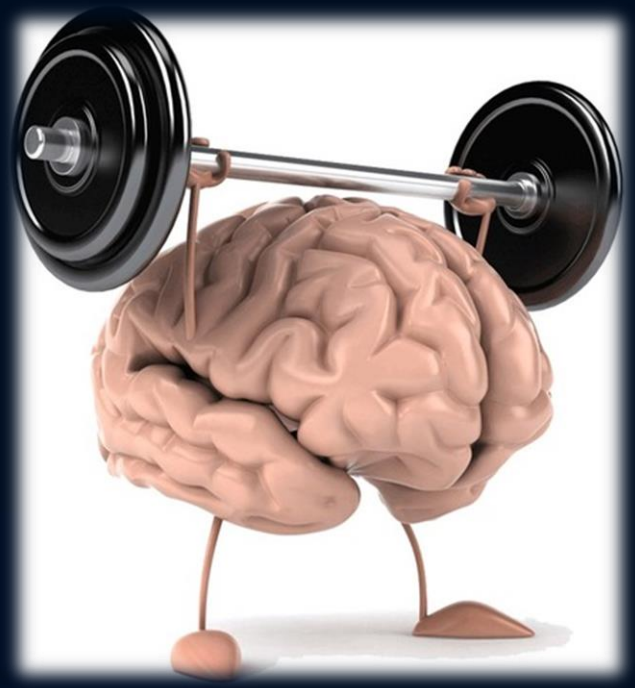
Insider attacks

- Spying
  - If a competitor wants to damage your organization, steal critical secrets or put you out of business, they just have to find a job opening, prepare someone to pass the interview, have that person hired, and they will be in the organization

- Corporate Espionage
  - Information theft & sabotage
- Revenge
  - It takes only one disgruntled person to take revenge and your company may be compromised
- Insider Attack
  - Most attacks occur "behind the firewall"
  - An inside attack is easy to launch
  - Prevention is difficult, thus the attack can easily succeed
  - Financial gain is a potential reason

Protecting yourself from SE attacks

- Slow down
- Research the facts
- Delete any requests for financial information or passwords
- Reject requests for help or offers of help
- Lie to security questions and remember your lies
- Beware of any downloads
- Secure your devices
- Follow security policies
- Don't let a link control where you land



http://bit.ly/tudydefcamp

Q&A

Tudor Damian

CEH, IT solutions specialist

www.tudy.tel