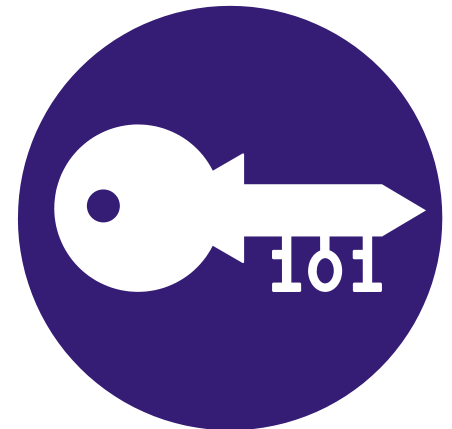
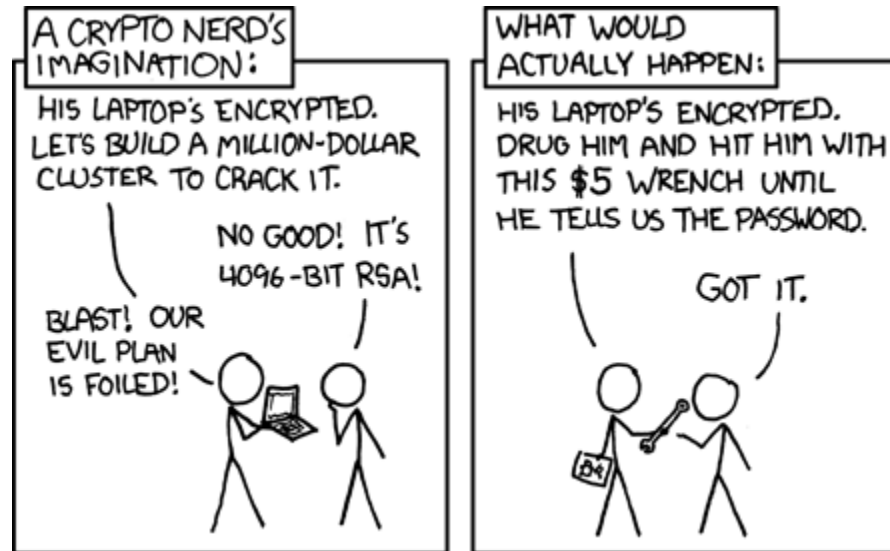


Social Engineering



Theory and practice



A parable



- Bank account
- Sales data / corporate strategy
- NASA's secret alien contact reports
- Credit card database
- Highly embarrassing self-insert Harry Potter fanfiction
- Nuclear launch codes

A parable



A parable

- Never sleeps
- Follows byzantine security policies to the letter
- Never gets bored, lazy or distracted
- Has no friends, lovers or fears
- Fast as lightning, strong as steel
- Requires specialist kung-fu to defeat



“The Machine”

A parable



Jeremy

- Works Wednesdays and Thursdays
- Hasn't read the employee handbook
- Balances spreadsheets while looking at memes
- Made of soft, squishy meat
- Answers social media quizzes titled "My top 10 fears and weaknesses"
- Happy to help anyone who drops him an email

A parable



Jeremy

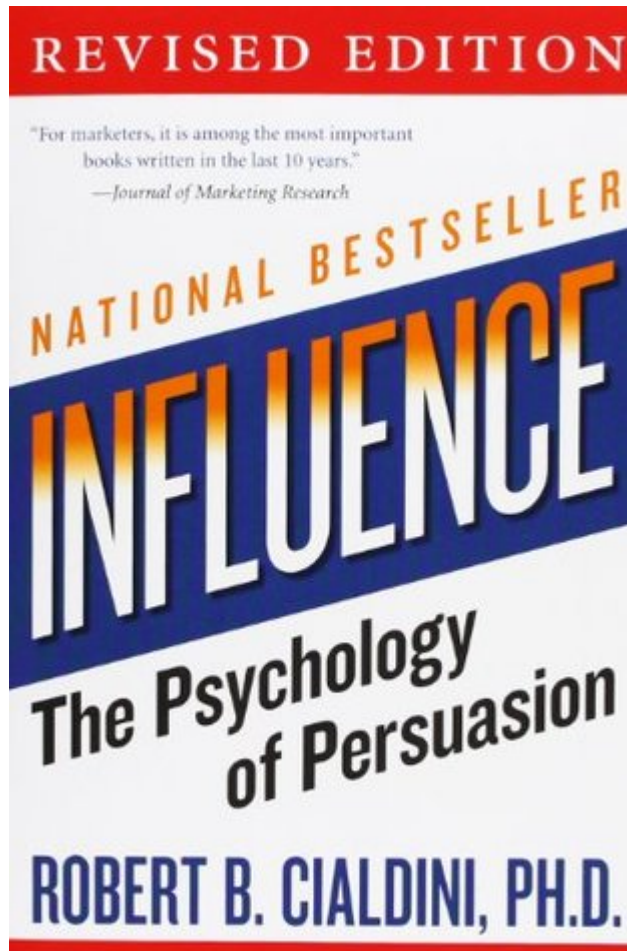


“The Machine”

Real-world social engineering

<https://www.youtube.com/watch?v=lc7scxvKQOo>

Principles of Persuasion



Heavily based on observations of salesmen

The 0th principle: perceived self-interest.

If you are offering something somebody wants, everything becomes easier.

Reciprocity



When someone gives us something we naturally want to repay them.

We can feel *obliged* to agree to whatever they ask of us.



Reciprocity



Our best price is £4,000

No way I can afford that.

Okay, I like you, so I've gone and talked to my boss, and he wasn't happy, but I think I can swing you a discount at £3,000

Well...



Commitment & consistency

When do you think people at a racetrack are more confident about their chosen horse winning?

1. Just before they place the bet?
2. Just after they have placed the bet?

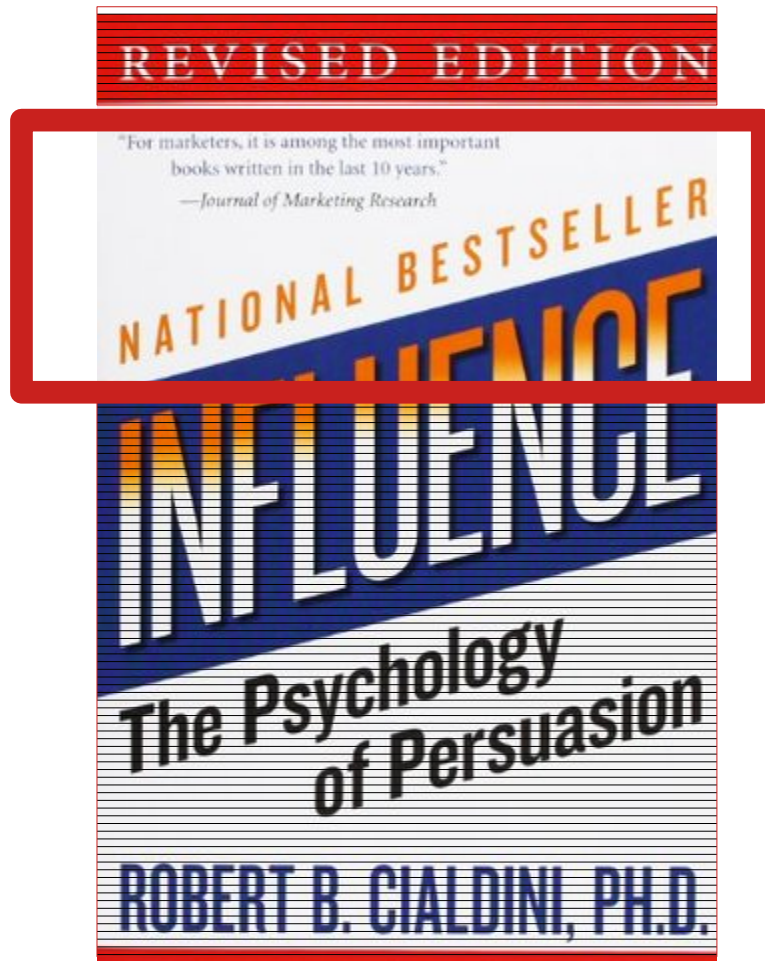
Commitment & consistency

If you can make someone “choose” something (even ‘temporarily’ or under protest), they are more likely to honor that commitment, and convince themselves that they always wanted it.

Desire to be seen to honor commitments is one of the most powerful motives in all of psychology.

”How are you today?”

Social proof



More than we would like to believe, we are 'herd animals' – we have a strong desire to fit in and do as others around us do, and we rely a lot on the judgements of our peers in making decisions.

Social proof

Asch's conformity test:
Which line is the same length?



Liking

Unsurprisingly, we trust people we like.

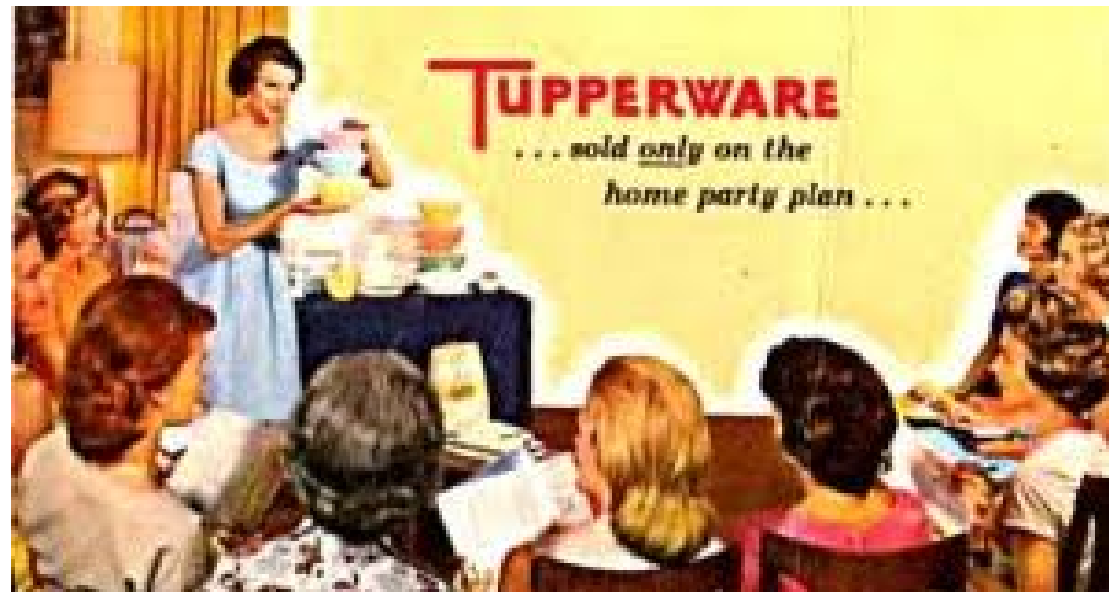
The 'halo effect': physically attractive people are more easily perceived as smart, sociable, funny, reliable, etc.



Liking

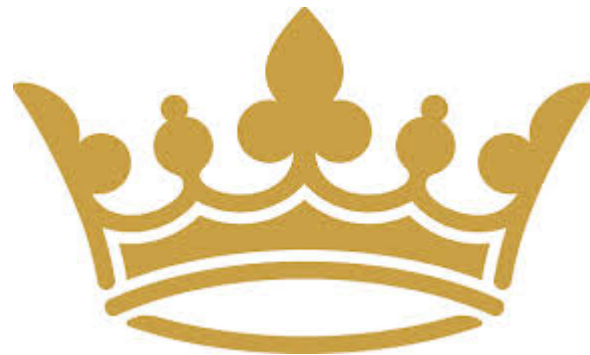
We also tend to like and trust people similar to ourselves

Scammers (like advertisers) often try to forge a 'personal connection' for this reason.



Authority

We do what people (who seem to be) in charge tell us to do.



Authority

- “My boss says...”
- “The lawyer wants...”
- “The bank needs...”
- “The board is insisting...”
- “HR are making us...”
- “The voters said...”

Scarcity



DEAL OF THE DAY

\$7.99 - \$89.99

Ends in 17:14:00

Save up to 40% on select Little Tikes preschool toys


★★★★★ 40

See details



Delivery

My billing address is in: **USA** | [Canada](#) | [Other Country](#)

Your tickets will be delivered via:

 **eTickets - Free!**

Get in with:

-  **Mobile**
Go mobile, the easiest way in! Just show your ticket on your phone.
-  **Print-at-Home**
Print your tickets and bring them to the event.

All orders are subject to credit card approval and billing address verification.

A [processing fee per order](#) is applied when applicable in addition to the [delivery price per order](#) listed above.

Continue

Buy these tickets before someone else does.



Scene from the cult classic 'Hackers'

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

Why does it work?

People are generally taught to be kind and helpful.
This is unfortunately easy to exploit.

Employees generally try really hard to do their job.
This includes working around any security policies that get
in the way.

People follow “common practice”, not theory.

Demographics

Are some people more likely to fall for scams/phishing than others?

Obvious point: someone with little computing experience will be less likely to pick up signs of a poorly made phishing site.

Agreeableness is one of the “big 5” psychological traits, and may well be correlated with phishing susceptibility – at least for people who are not educated about security.

African princes

I AM JOHNSON SAVIMBI FROM ANGOLA.MY LATE FATHER GENERAL JONAS SAVIMBI WAS THE REBEL LEADER WHO CONTROLLED THE GOLD AND THE DIAMOND REGIONS OF ANGOLA FOR 27 YEARS SUCCESSFULLY WITHOUT INTERNAL OR EXTERNAL INTERFERENCE ...

... THE FIRST BOX CONTAINS 200KG OF 22 KARRAT ALLUVIA GOLD DUST WHILE THE SECOND BOX CONTAINS (\$40 MILLION U.S. DOLLARS).THESE TWO BOXES ARE UNDER THE CUSTODY OF A SECURITY COMPANY HERE IN COTONOU, BENIN FOR PROTECTIVE SAFEKEEPING PURPOSES ...

PLEASE SIR,I WANT YOU TO HELP ME TRANSFER THIS PHYSICAL CASH INTO YOUR BANK ACCOUNT ... I AM READY TO SIGN AN UNDERTAKING TO RELEASE 20% OF THIS TOTAL MONEY TO YOU

African princes

Very few people would fall for such a story.

According to a paper by Microsoft Research, that is exactly the point!

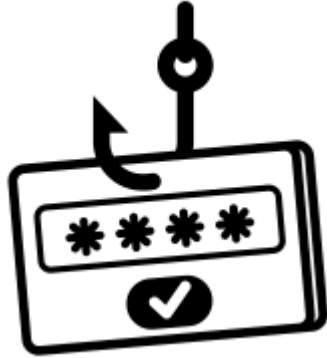
Before they can scam someone, the criminals have to set up a trust relationship, make some small transfers so as to not set off the banks' fraud alarms, etc.

So they want to filter for “complete suckers” to start with.

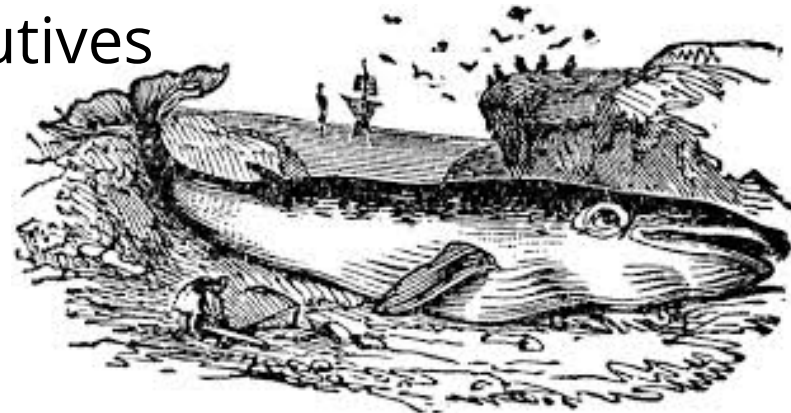
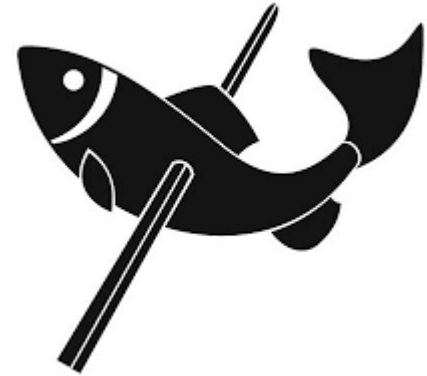
Wasting their time could be very effective!

Phishing

Phishing



- **Phishing:** tricking people into handing over confidential data, usually username/password
- **Spear phishing:** targeting particular individuals
- **Whaling:** targeting senior executives or VIPs




Phishing

Gmail ▾


← + ! 🗑️ 📁 🏷️ 📧 ▾

Important: Your Password will expire in 1 day(s) 📧 Inbox x 🖨️ 📧

 **MyUniversity** 12:18 PM (50 minutes ago) ☆ ↩️ ▾
to me ▾

Dear network user,

This email is meant to inform you that your MyUniversity network password will expire in 24 hours. Please follow the link below to update your password myuniversity.edu/renewal


MY UNIVERSITY

Thank you
MyUniversity Network Security Staff

Phishing

```
<a href="phishingsite.com">google.com</a>
```

This is how you write a link in HTML.

The contents of the tag (here: google.com) is what is displayed to the user.

The "href" is where the link sends you.

With JavaScript, you can even change the link contents during a click, so "hovering" won't show the fake destination (facebook does this to help it track you).

Phishing sites

Phishing sites are usually short-lived and taken down within days if not hours.

They can still be profitable if attackers target a lot of people before the site gets caught.

Phishing sites are often hosted

- on legitimate sites, by hacking into the site
- on self-hosting/cloud providers
- on domains bought with stolen cards.

Safe Browsing



Deceptive site ahead

Attackers on **testsafebrowsing.appspot.com** may trick you into doing something dangerous like installing software or revealing your personal information (for example, passwords, phone numbers or credit cards). [Learn more](#)

Automatically send some [system information and page content](#) to Google to help detect dangerous apps and sites. [Privacy Policy](#)

DETAILS

Back to safety

Not a good idea

One user: *"I just type in my password anyway. If it's not the real site, they won't know what to do with it."*

Similar mistake: *"I first type in a fake password. If the site doesn't accept it, I know it must be the real site."*

In a **man-in-the-middle** attack, the site both records what you type and passes it on to the real site – that way they can check if your password is correct or not.

A good idea?

"I check if the site looks ok, you know, has the right logos and things ..."

If something looks dodgy (e.g. full of bad grammar), that is a warning sign.

But looking ok is not proof that the site is legitimate.

A properly done phishing site looks exactly like the real thing!

General advice

Treat any e-mail with suspicion that asks you to click a link to log in to a service where you already have an account.

It is safer to open a browser, log in to the site directly and then to find whatever you need to do (if it's a "new message", the site will presumably tell you).

Exceptions: many sites legitimately use links for confirming your e-mail address when you create a new account, and to reset your password if you forget it.

General advice

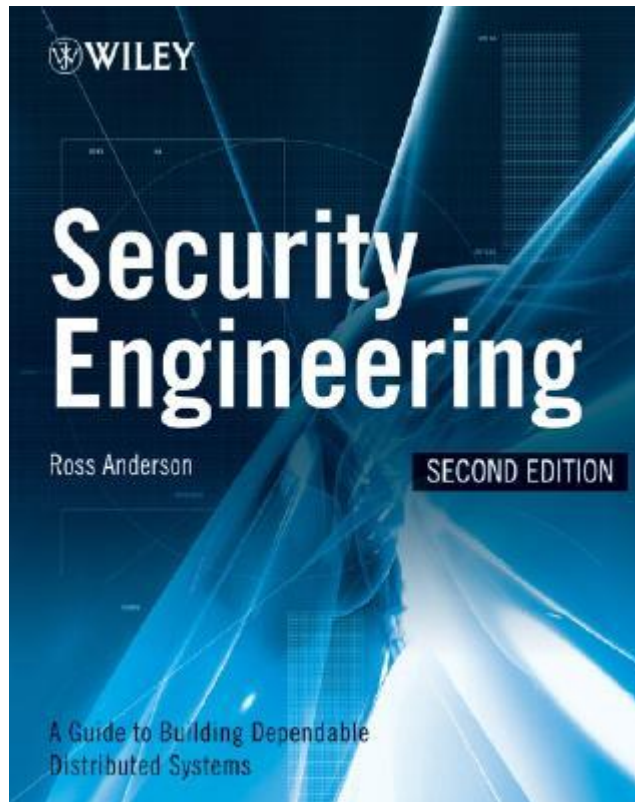
Never use a debit/credit card PIN number on anything other than an ATM or a bank-provided card reader.

The PIN is never required online or over the phone.

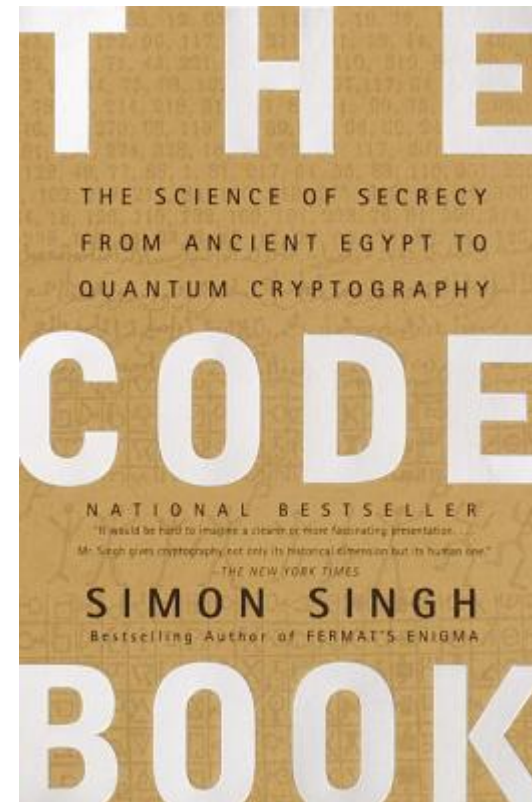
Do not give out your password, or particular letters of your password, over the phone unless you're on a service that really does use this silly authentication method.

The University of Bristol does not do this!

Further reading



Security Engineering
Ross Anderson



The Code Book
Simon Singh