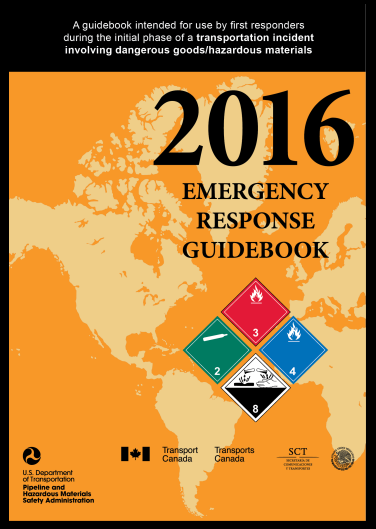
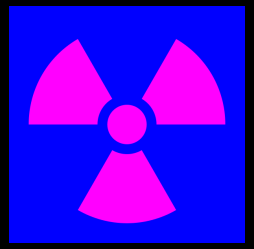
Prepare for the worst

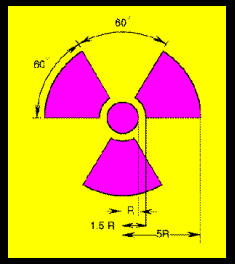
because that device is deadly



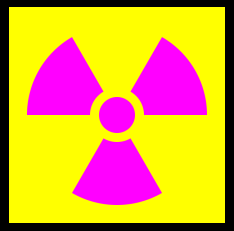
Dr. Sunny Fugate
Research Scientist
sunny.fugate@gmail.com

Ionizing Radiation

1946 

1948 

- Blue background was abandoned due to poor visibility
- 1950's experimented with various kinds of arrows, but the original was still the winner by popular selection

1950's   

International symbol 

2007 

supplemental warning symbol to indicate sealed ionizing radiation source

[1] http://www.freesoftwhere.org/2016/05/31/trefoils-past/
[2] Radiation Warning Symbol (Trefoil), Oak Ridge Associated Universities, http://www.orau.org/ptp/articlesstories/radwarnsymbstory.htm
[3] https://en.wikipedia.org/wiki/Hazard_symbol

Biological

1966

'We tested the sample symbols across the country -- the marketing department had survey groups to test different labels for Dow products. There were half a dozen of our original symbols in this survey of 24 different symbols. The rest were recognizable, like the peanut man for Planter's peanuts, the Texaco star, the Shell Oil symbol, the Red Cross and the swastika. They were asked to look at them and then asked to guess at what each one meant. The biohazard symbol got the fewest guesses. Then we went back one week later to the same set of people and the same set of symbols, plus 36 more common ones, and asked them which of these did they remember the best. And they picked out the biohazard symbol." Charles Baldwin [1]

[1] http://web.archive.org/web/20110716160837/http://www.hms.harvard.edu/orsp/coms/BiosafetyResources/History-of-Biohazard-Symbol.htm

Warning Signs

Common warning signs

Toxic

Harmful

Oxidizer

Explosive

Flammable

Corrosive

[1] Warning Signs, Wikipedia, Retrieved 13 Oct 2016, https://en.wikipedia.org/wiki/Warning_sign
[2] GHS Hazard Pictograms, Retrieved 13 Oct 2016, https://en.wikipedia.org/wiki/GHS_hazard_pictograms

Warning Signs

Uncommon warning signs

Australia:
Tasmanian devil
crossing

Netherlands:
quicksand

Finland:
mosquito swarms

Greenland:
dogsled crossing

[1] Warning Signs, Wikipedia, Retrieved 13 Oct 2016, https://en.wikipedia.org/wiki/Warning_sign
[2] GHS Hazard Pictograms, Retrieved 13 Oct 2016, https://en.wikipedia.org/wiki/GHS_hazard_pictograms

Pop-culture

Dilution

"…I ran into a peculiar situation one time a couple years ago when someone was putting on a seminar on biohazards. As gifts for the participants, he devised a beautiful tie with little biohazard symbols all over it. This got me upset, and I sent him kind of a nasty letter saying this symbol was not designed to be used sartorially."" Charles Baldwin [1]

[1] http://web.archive.org/web/20110716160837/http://www.hms.harvard.edu/orsp/coms/BiosafetyResources/History-of-Biohazard-Symbol.htm

Pop-culture

Misuse

Pop-culture

Misuse

Pop-culture

Appropriate use in art, games, film can educate as well

A cyber warning trefoil

Why?

- Indirect harm
  - Loss of data
  - Loss of resources energy, money, respect
- Direct harm
  - Industrial control and SCADA systems
  - Computer controlled vehicles
  - Exploding batteries
  - Prosthetics — future sophisticated computer controlled/mediated limbs
  - Implants (pacemaker, cochlear implant, future artificial organs)
- Examples? — Science Fiction provides plenty

Informed by popular culture

and speculative science fiction

Today

Thumb-drives with malware

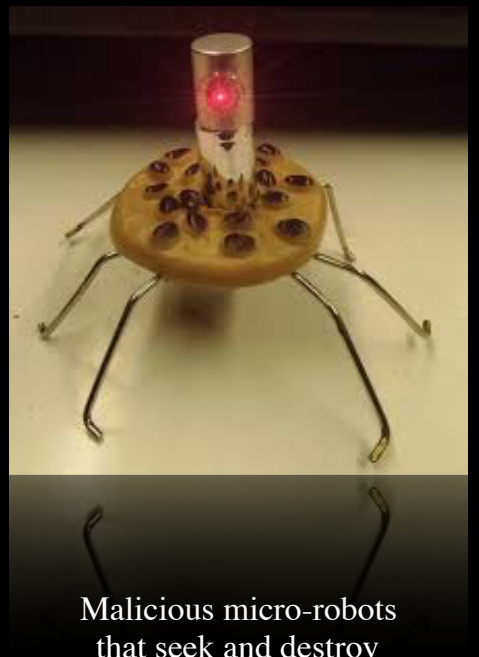
Tomorrow

?

Today

Thumb-drives with malware

Tomorrow



Malicious micro-robots
that seek and destroy

Today

Exploit development is hard

Tomorrow

?

Today

Exploit development is hard

Tomorrow

Exploit breeding and husbandry
for fun and profit

Today

Quadcopters with firearms

Tomorrow

?

Today

Quadcopters with firearms

Tomorrow

ED-209 with firearms and bad software

Today

Self-driving cars

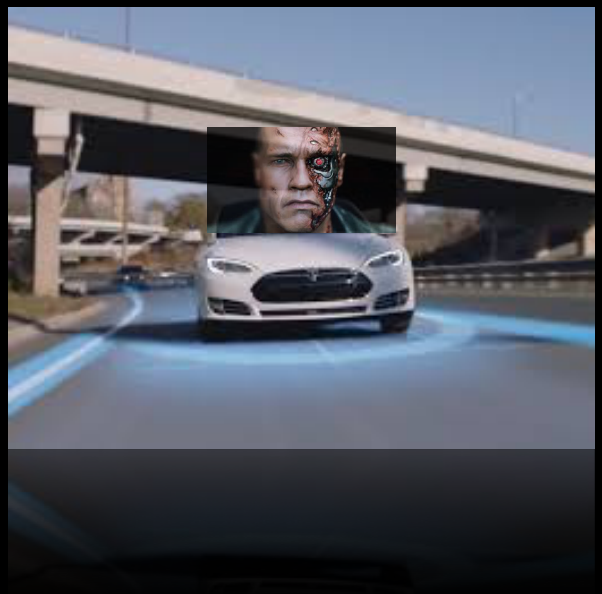
Tomorrow

?

Today

Self-driving cars

Tomorrow



the Model ST-800

Today

Memes and thought vireo are fun and stupid

Tomorrow

?

Today

Memes and thought vireo are fun and stupid

Tomorrow

Losing your mind Ghost-in-the-Shell-style

Today

Love dolls are creepy

Tomorrow

?

Today

Love dolls are creepy

Tomorrow

Androids and the uncanny abyss of malicious electric sheep

Today

Zombies aren’t real

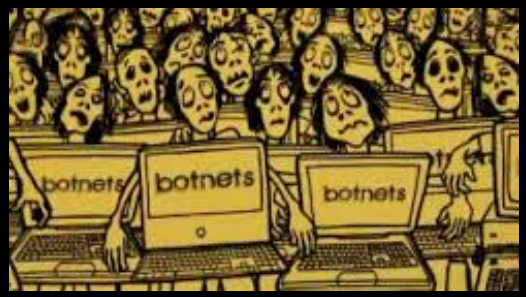
Tomorrow

?

Today

Zombies aren’t real

Tomorrow

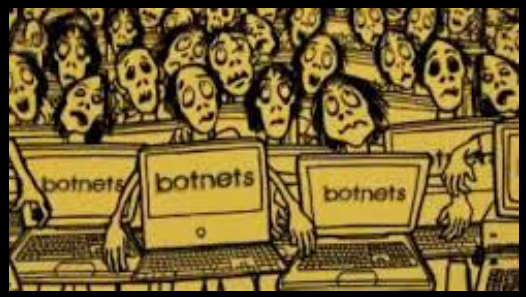


Zombies are real when they are robots

Today

Zombies aren’t real

~~Tomorrow~~
Today



Zombies are real when they are robots

So what do we have now?

A cyber warning trefoil

So what do we have now?
— Just a hodgepodge of computer security warning icons and pop culture art

A cyber warning trefoil

In what ways can I use the Internet while avoiding its risks?

DISCUSSION | Feb 25, 2015

by: 20schiffinor

keywords: avoiding the dangers of the internet | cyber bullying | cyber safety | identity theft protection | malware protection

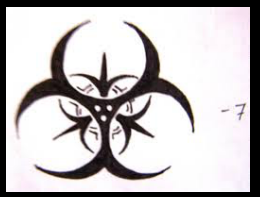
channels: from the middle (6–8)

Most people use the Internet every day for either work or recreational reasons. However around 2 million people suffer of a cyber attack monthly whether it be Identity theft or an unresponsive computer. Malware verymuch plays a role in our daily lives our computers protections and firewalls encounter them almost daily, but from time to time our computers may not catch or stop the viruses that constantly bombard our computers. Therefore it is our responsibility to steer clear of these dangerous and/or annoying things. This malware can be found in a innocent thing like looking up the date a movie came out to something not as innocent like watching a illegally downloaded movie. No computers protection is perfect and a well made virus or trojan can bypass most and all security on your computer if you force download it or it finds a loophole.

Add new comment Share

Very close to biohazard trefoil

and related pop-art



Source: http://youthvoices.net/discussion/what-ways-can-i-use-internet-while-avoiding-its-risks-18

A cyber warning trefoil

Designed by the creators of DigiMon?

A cyber warning trefoil

DIGIMON WIKI

On the Wiki | General | Anime | Other | Comm

Wiki Activity | Random page | Videos | Images

Digital Hazard

7,699 PAGES ON THIS WIKI

Edit this page | Talk 8

The **Digital Hazard** symbol appears on the bodies of certain Digimon. According to *Digimon Tamers*, the presence of this symbol means that the Digimon has the potential to be highly destructive, and, if corrupted, could threaten the very existence of both the Digital World and the Human World.[*citation needed*] The symbol bears a striking similarity to that which indicates a biohazard.

The trefoil **Digital Hazard** symbol.

Source: http://digimon.wikia.com/wiki/Digital_Hazard - Retrieved 8 Oct 2016

A cyber warning trefoil

of cyber warning symbols

Problems:

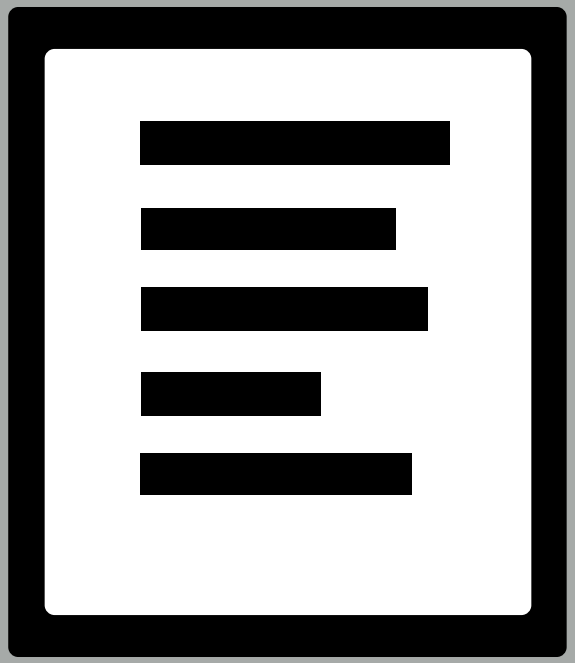
- Popular culture use
- It doesn't mean anything for our purposes
- Not culturally associated with our kinds of "digital monsters"
- Copyright

Properties of a good warning symbol

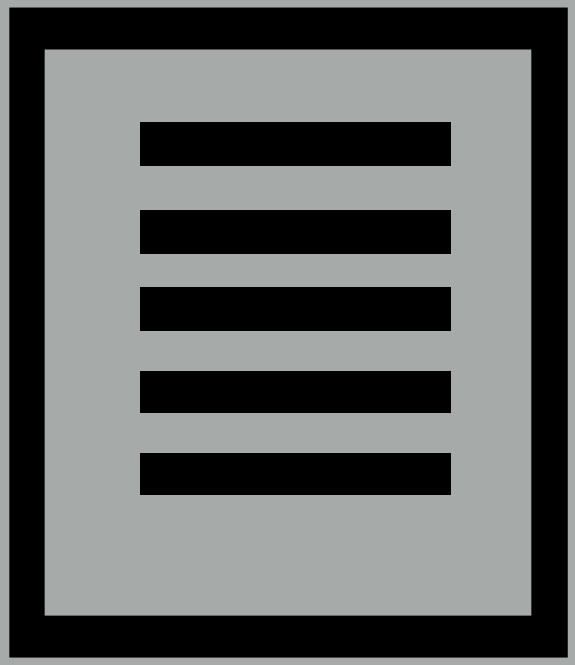
- Follows recognizable warning tre-foil pattern
- Visible at small and large scale
- Visible in many lighting conditions
- Recognizable after partial destruction
- Distinguishable from other warning symbols
- Easy to recreate, draw, stencil
- Accepted by the community
- Free use

Design

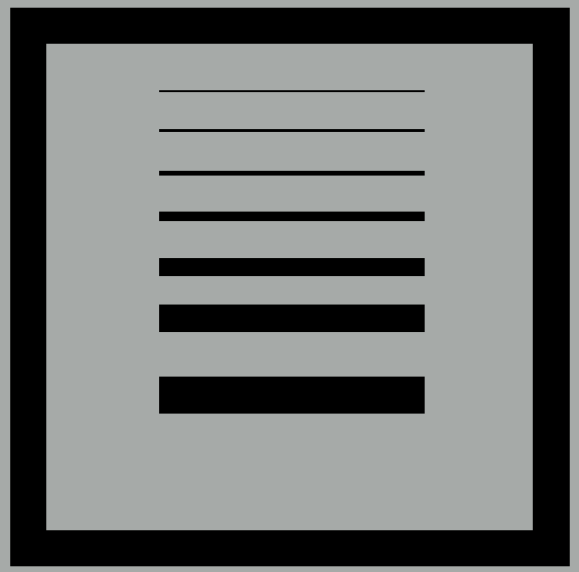
A lonely icon. Just a file, or some data, or a program, in the abstract



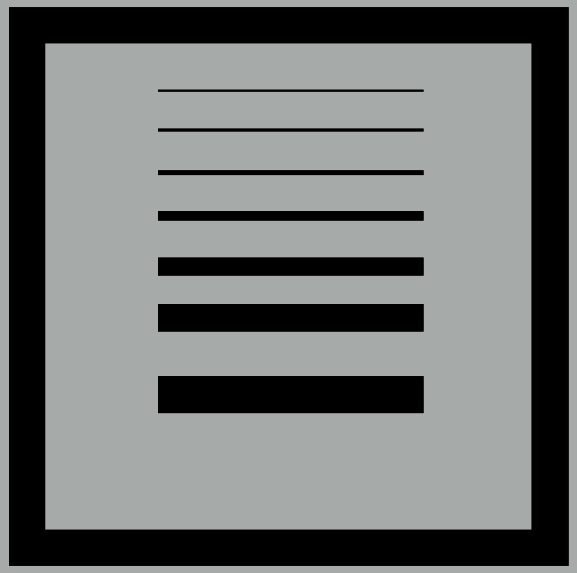
bigger



simpler



idea of data we cannot easily see, not just readable data, but encoded, encrypted, obfuscated



a couple of 60 degree rotations

You can’t help but make triangle looking things when making a trefoil

The malicious data interconnects, has C2 channels, has structure, possibly centralized control

The malicious data isn’t contained… it affects the surrounding computing environment.

It radiates outward just as the radiating blocks of the ionizing radiation symbol imply.

Final symbol ready for use as a stencil

Criteria for use?

For any device/data/software, ask the following:

(A) Test of trust

Do you trust the source and contents?

(B) Test of intent

Is it intended to cause harm?

(C) Test of harm

Will it cause harm? Can it cause harm?

(D) Test of trial

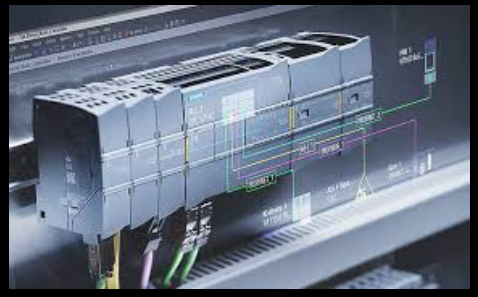
Could it be easily forced to cause harm?

Where to use

- In any situation in proper association with malicious data, algorithms, or devices.
  - Computing devices
  - Software
  - Data
  - Signals
  - Art, Media, Film depicting proper labeling of the above

(potentially) Deadly Devices

USB Killer



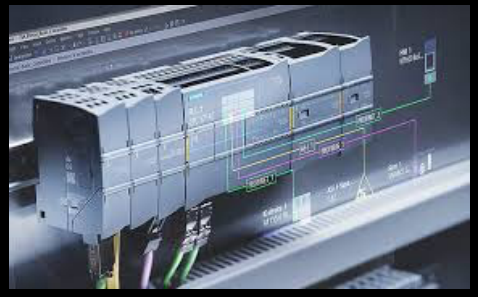
WiFi Pineapple

Any device with the potential to be deadly is an appropriate use?

Why the use of the term “potential”? Because handguns aren’t deadly when used as a deterrent, but they are still potentially deadly. A biological agent is perfectly safe when proper safeguards are taken. A radiological hazard is safe when contained within sufficient and proper shielding.

(potentially) Deadly Devices

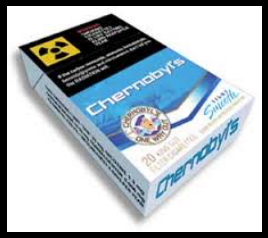
USB Killer



WiFi Pineapple

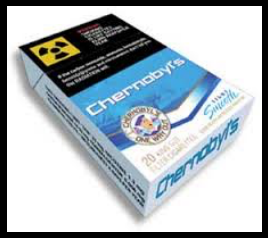
Where absolutely not to use

- If you have to ask….
  - Can I put this on a t-shirt?
  - Use it to label my smokes?
  - On something that floats?
  - For a sick tattoo?



Where absolutely not to use

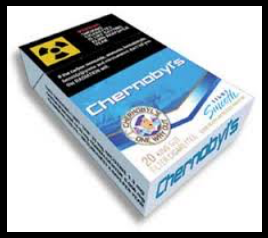
- If you have to ask….
  - Can I put this on a t-shirt?
  - Use it to label my smokes?
  - On something that floats?
  - For a sick tattoo?



Sure

Where absolutely not to use

- If you have to ask….
  - Can I put this on a t-shirt?
  - Use it to label my smokes?
  - On something that floats?
  - For a sick tattoo?



Surely not.

What else?

- The symbol itself shouldn't be deadly or dangerous
  - Warning symbols are precursors to threats

What else?

- The symbol itself shouldn't be deadly or dangerous
  - Warning symbols are precursors to threats

I shouldn't be infected by a biological agent just by viewing or coming into contact with the biohazard symbol itself.

What else?

- The symbol itself shouldn't be deadly or dangerous

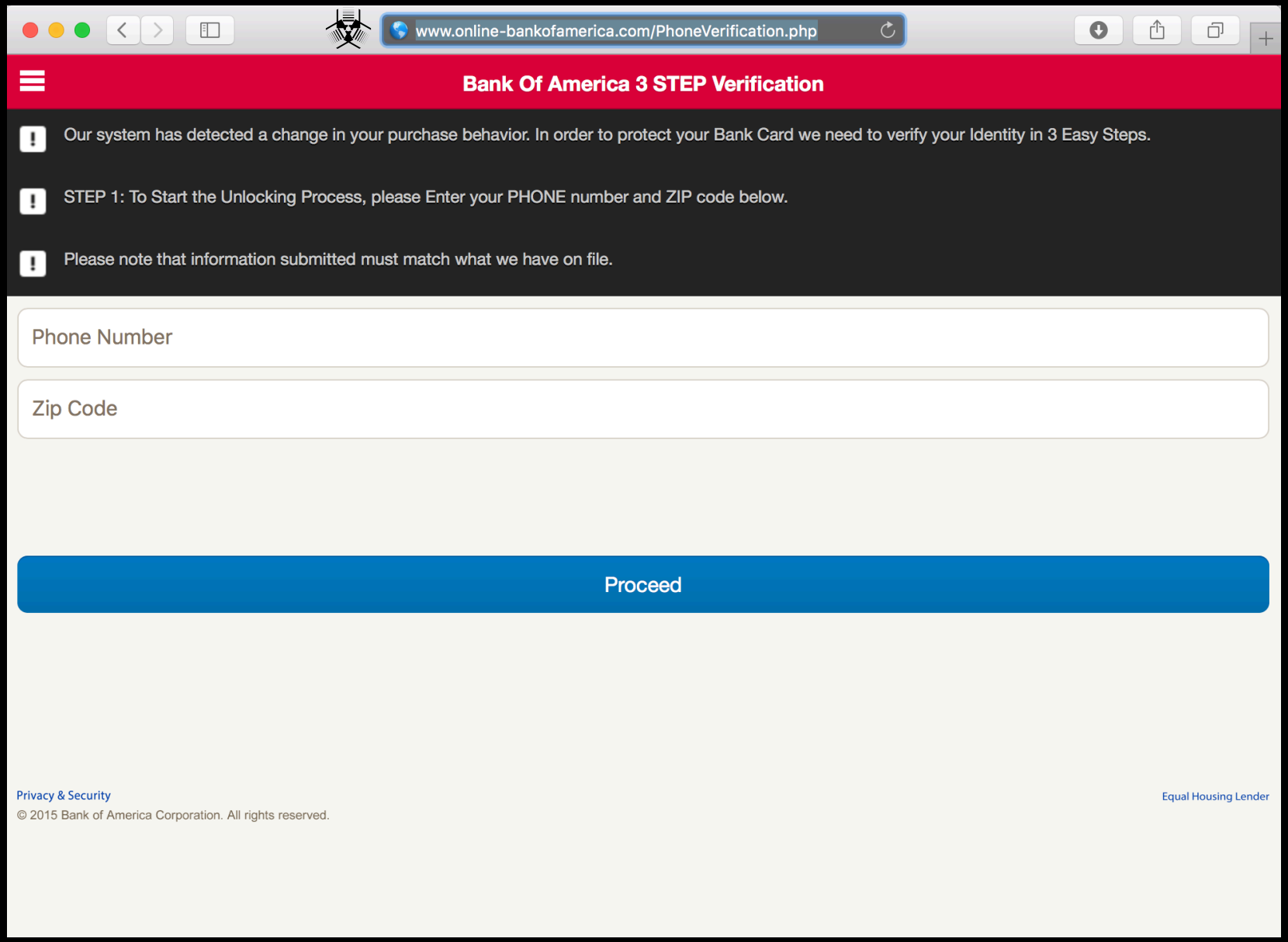
these guys are exceptions



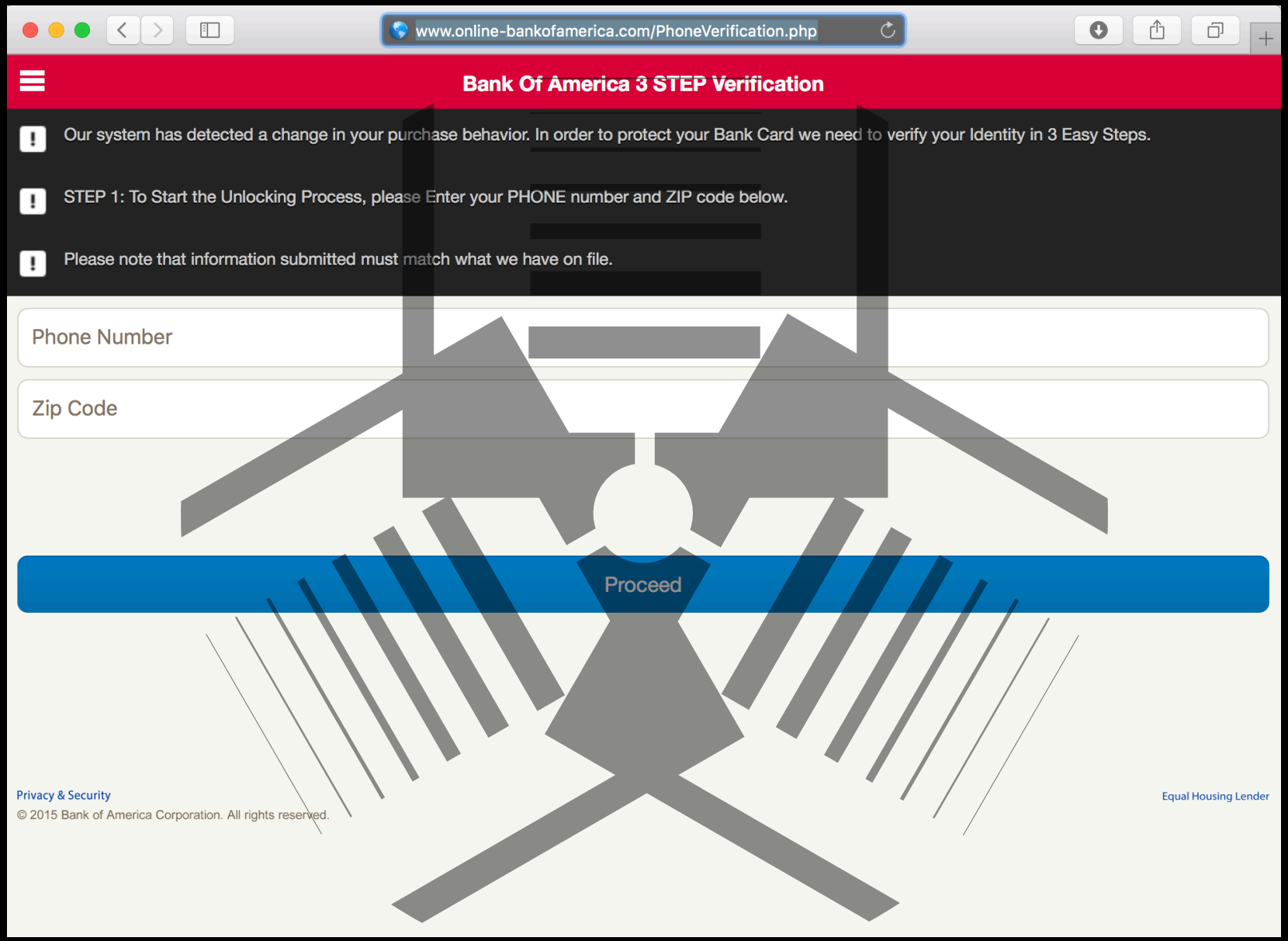


Example Uses

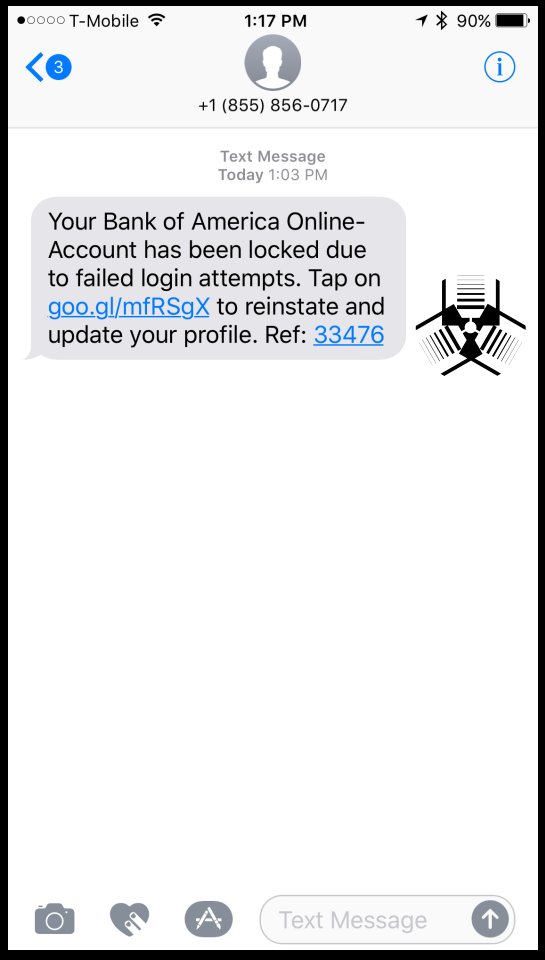
Safe(r) Browsing



Safe(r) Browsing

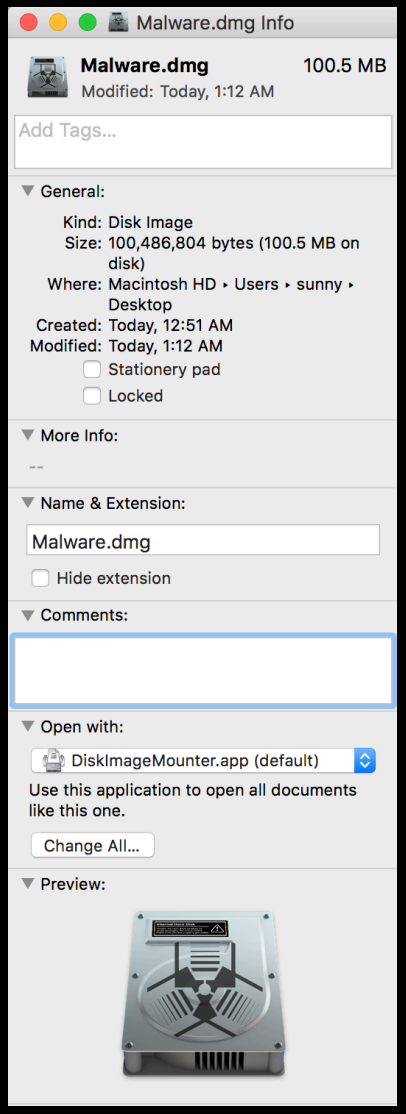


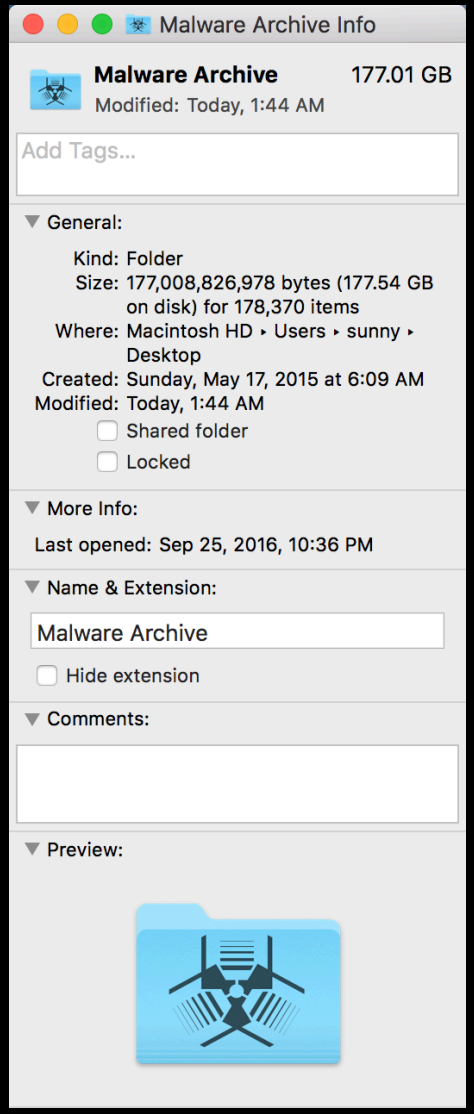
SMShing with trefoils



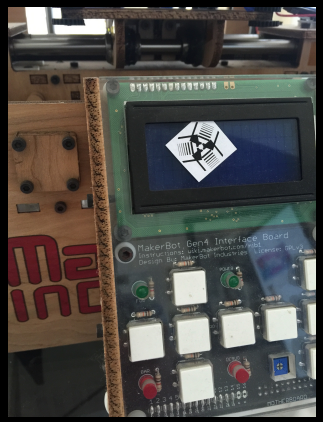
This was an actual SMS phishing attempt sent to my phone

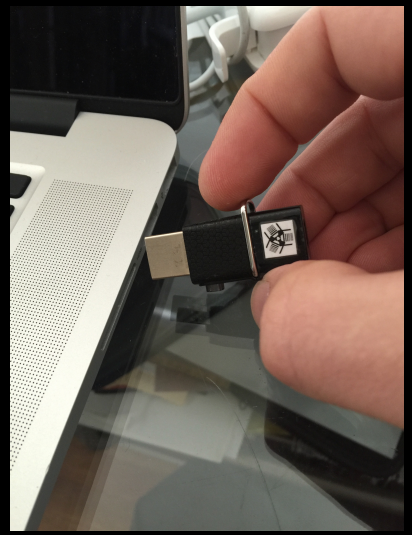
Files, folders, and disks with trefoils

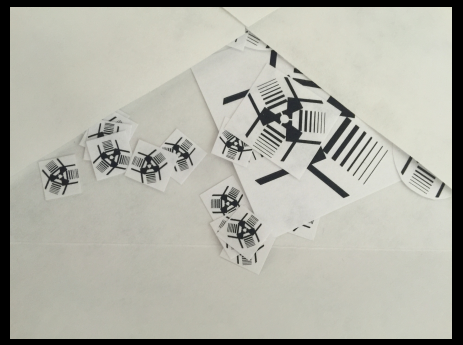




Labeling Devices







Labeling Devices

Trefoil should be placed in a prominent location

Don’t do this

It will confuse your kids

dad, what am I listening to?

Don’t do this either

The stickers are really difficult to remove afterward

and it makes task switching impossible

And this….

And this….

is like the opposite of a baby-on-board decal

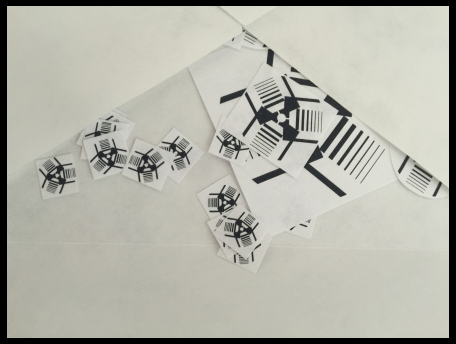
And this….

It will also confuse your kids

Making Stickers

Print

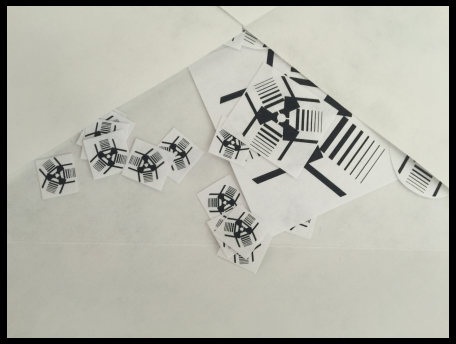
Cut



Paste

Print

Cut



Paste

Glue, scotch tape, mod podge, spit, …

A small experiment

What do we do when the threat is invisible?

Biological and radiological threats have taught us something crucial.

If we can’t see it…. that doesn’t mean it isn’t there or can’t have an effect.

Broadcast that its bad

Broadcast that its bad

on a network
in a packet

RFC 3514

just a bit of evil

Network Working Group
Request for Comments: 3514
Category: Informational

S. Bellovin
AT&T Labs Research

1 April 2003

The Security Flag in the IPv4 Header

Status of this Memo

This memo provides information for the Internet community. It does not specify an Internet standard of any kind. Distribution of this memo is unlimited.

Abstract

Firewalls, packet filters, intrusion detection systems, and the like often have difficulty distinguishing between packets that have malicious intent and those that are merely unusual. We define a security flag in the IPv4 header as a means of distinguishing the two cases.

1. Introduction

Firewalls [CBR03], packet filters, intrusion detection systems, and the like often have difficulty distinguishing between packets that have malicious intent and those that are merely unusual. The problem is that making such determinations is hard. To solve this problem, we define a security flag, known as the "evil" bit, in the IPv4 [RFC791] header. Benign packets have this bit set to 0; those that are used for an attack will have the bit set to 1.

1.1. Terminology

The bit field is laid out as follows:

```
 0
+-+
|E|
+-+
```

Currently-assigned values are defined as follows:

0x0 If the bit is set to 0, the packet has no evil intent. Hosts, network elements, etc., SHOULD assume that the packet is harmless, and SHOULD NOT take any defensive measures. (We note that this part of the spec is already implemented by many common desktop operating systems.)

0x1 If the bit is set to 1, the packet has evil intent. Secure systems SHOULD try to defend themselves against such packets. Insecure systems MAY chose to crash, be penetrated, etc.

3. Setting the Evil Bit

There are a number of ways in which the evil bit may be set. Attack applications may use a suitable API to request that it be set. Systems that do not have other mechanisms MUST provide such an API; attack programs MUST use it.

Multi-level insecure operating systems may have special levels for attack programs; the evil bit MUST be set by default on packets emanating from programs running at such levels. However, the system MAY provide an API to allow it to be cleared for non-malicious activity by users who normally engage in attack behavior.

Fragments that by themselves are dangerous MUST have the evil bit set. If a packet with the evil bit set is fragmented by an

RFC 3514

just a bit of evil

If it isn't there, it might still be bad.

RFC 3514

just a bit of evil

It it is there, it is going to be either evil

RFC 3514

just a bit of evil

It it is there, it is going to be either evil
or stupid

RFC 3514

just a bit of evil

It it is there, it is going to be either evil
or stupid
or both.

Inside a packet isn’t the only kind of invisible

Inside a packet isn’t the only kind of invisible

What about RF maliciousness?

Maybe we can just broadcast that it’s bad?

Maybe we can just broadcast that it’s bad?

But where?

in the physical layer?

Broadcast that its bad

Can we do this using signal modulation?

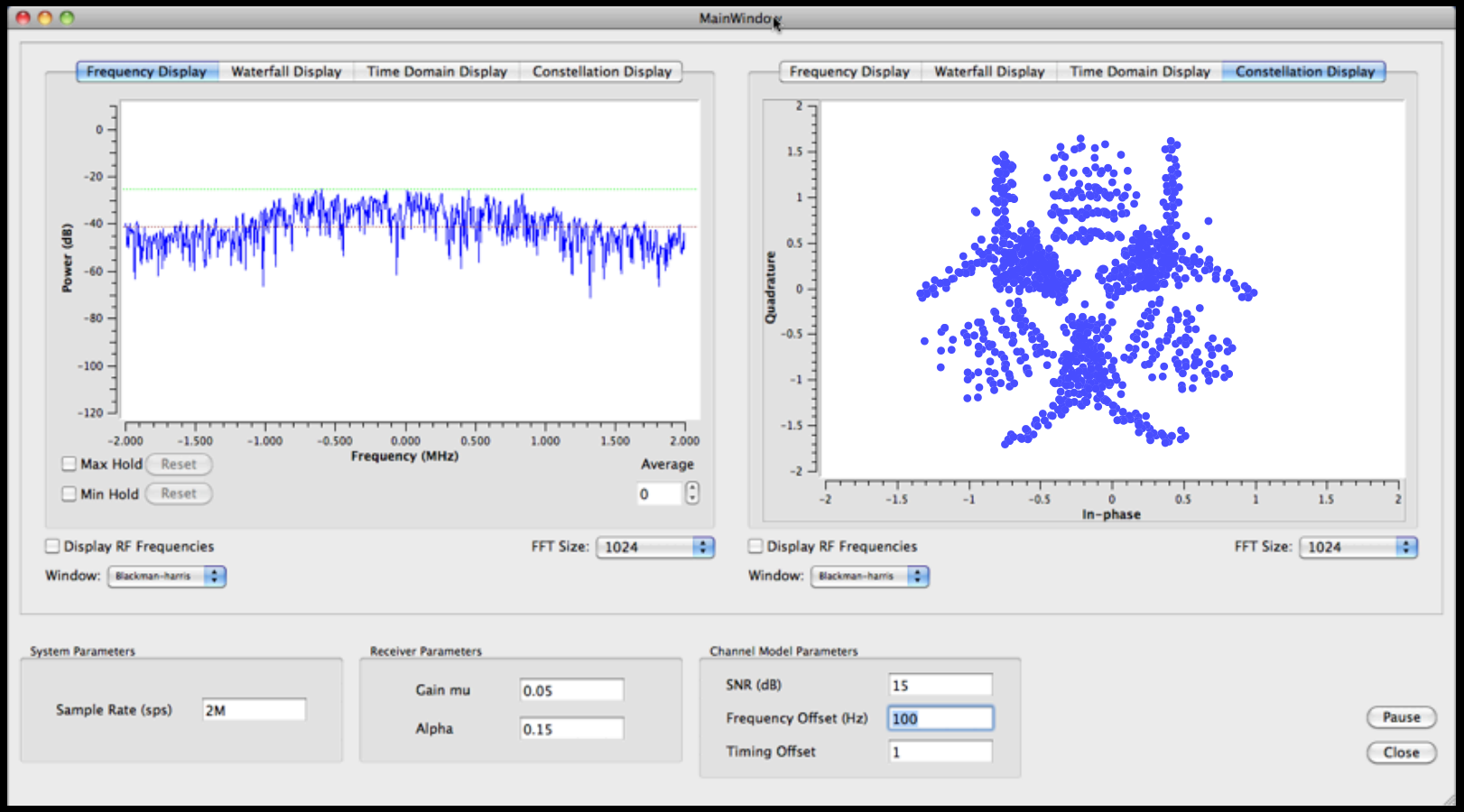
On the transmitter (Modulating the points onto a radio signal):

1. Make the X,Y coordinates a series where the series is normalized between -1 and +1
2. A digital radio can transmit a complex number, which is referred to as the in-phase and quadrature components, or I and Q. (how this is done is beyond the scope of this talk)
3. I and Q correspond to X,Y when viewed on a cartesian plot
4. Configure the radio (probably a software defined radio) to transmit raw I,Q values, as opposed to an actual modulation (such as QPSK or FSK)
5. Feed in the series of I,Q points to the radio

On the receiver:

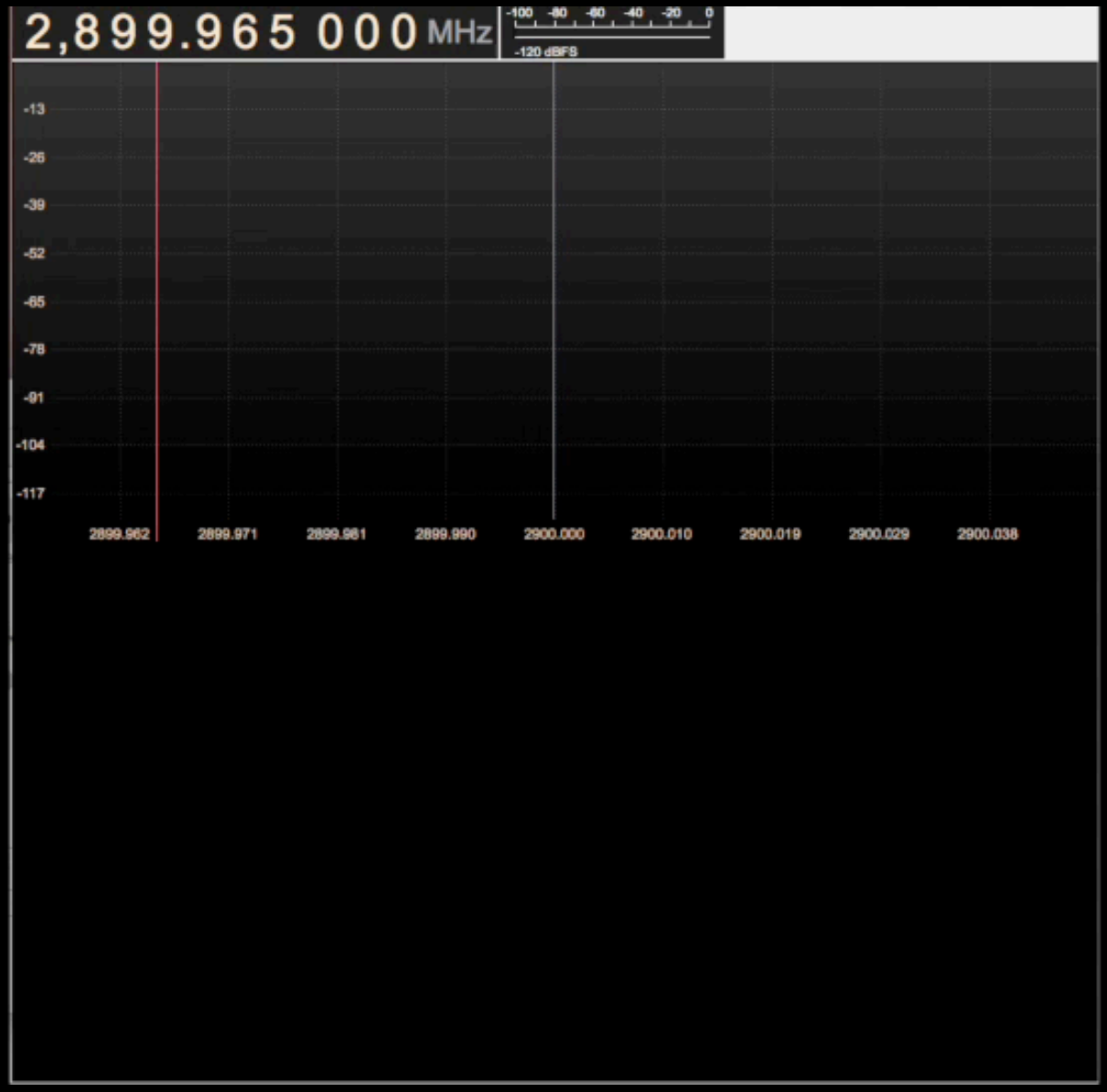
1. Configure the receiver to plot the I,Q values received, with a history of some number of points (the number of points that made up the original image)
2. Receiver will need to have its frequency and internal oscillator exactly match the transmitter
3. Show your boss the warning sign over the radio's physical layer

Broadcast that its bad

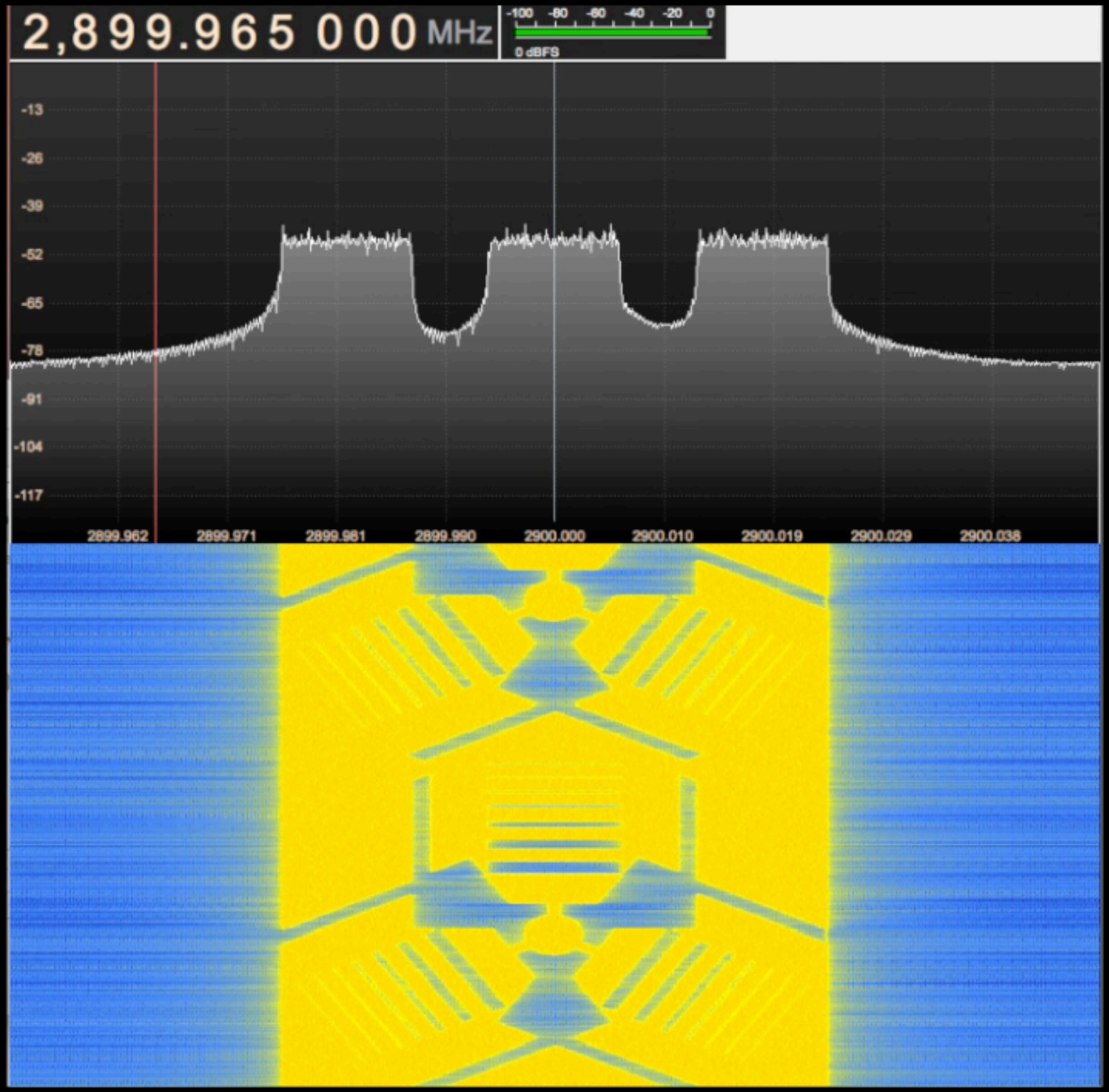


Evil-IQ?

An even easier label for malicious RF



An even easier label for malicious RF



License

- Creative Commons License
- Attribution-ShareAlike 4.0 International

This means use it wherever and however you want, modify it, etc but just attribute the original source and share alike.

Also, if you can, let me know how you are using it!

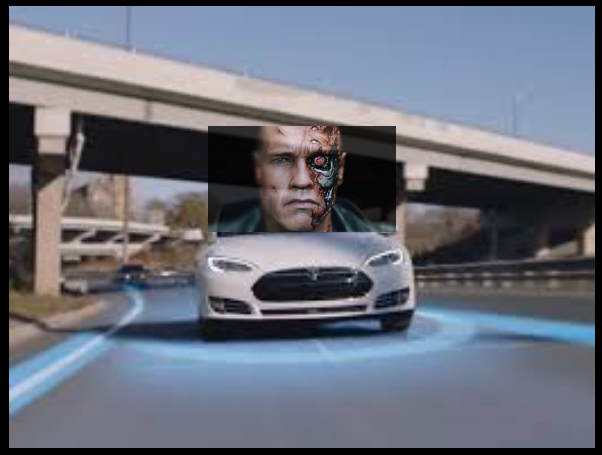
http://creativecommons.org/licenses/by-sa/4.0/

So....

Model T-800

because this guy

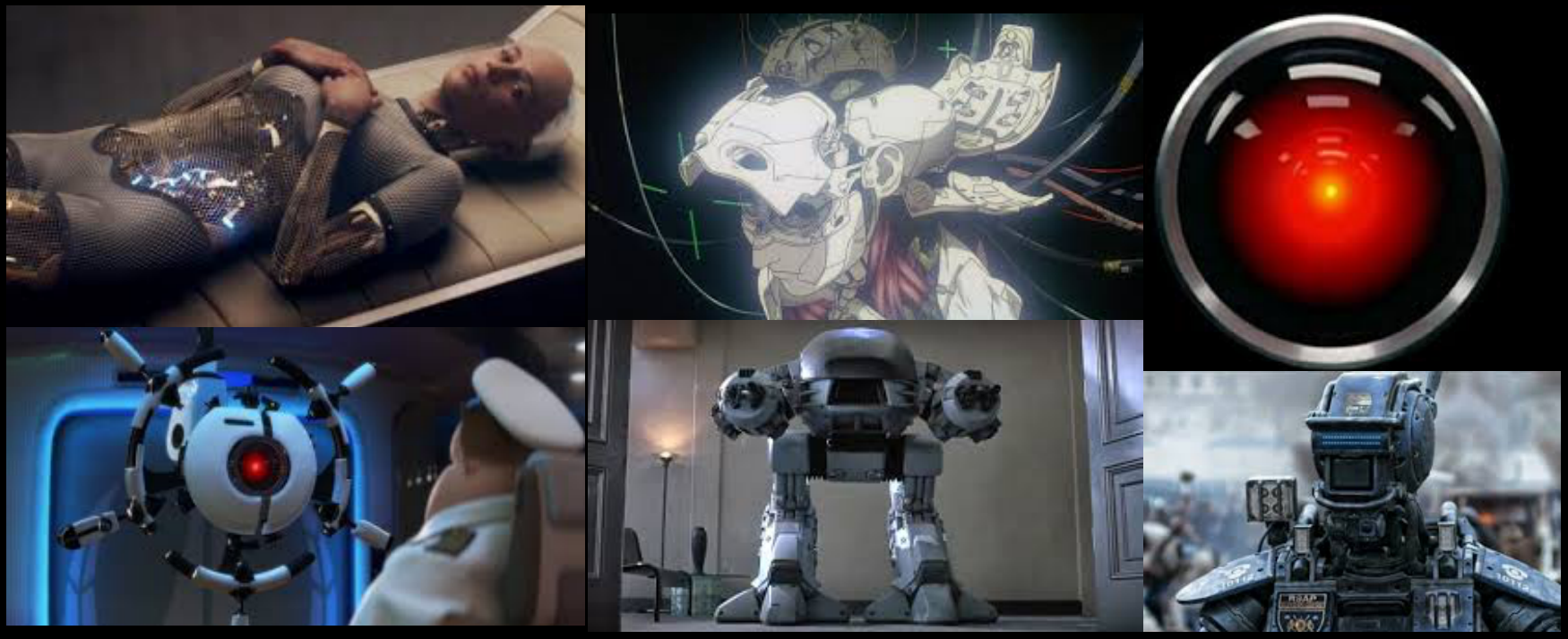
and these guys



Model ST-800?

EduDrive-209?

and all of these



may be coming to a future near you

and all of these

are already here

We need a better label

for bad

Thanks