Argonne
NATIONAL
LABORATORY

... for a brighter future

VAT

U.S. Department
of Energy

UChicago ▸
Argonne LLC

A U.S. Department of Energy laboratory
managed by UChicago Argonne, LLC

Presentation for the ASIS International Annual Meeting
Anaheim, CA, September 21-24, 2009

287 Security Blunders You Should Avoid

Jon S. Warner, Ph.D.
Roger G. Johnston, Ph.D., CPP

Vulnerability Assessment Team
Argonne National Laboratory

630-252-6168 rogerj@anl.gov
http://www.ne.anl.gov/capabilities/vat

Vulnerability Assessment Team (VAT)

Sponsors

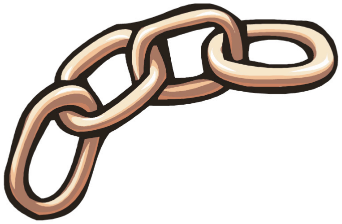
- DHS
- DoD
- DOS
- IAEA
- Euratom
- DOE/NNSA
- private companies
- intelligence agencies
- public interest organizations

The VAT has done detailed vulnerability assessments on hundreds of different security devices, systems, & programs.

A multi-disciplinary team of physicists, engineers, hackers, & social scientists.

> The greatest of faults, I should say, is to be conscious of none.
> -- Thomas Carlyle (1795-1881)

Weakest Link Theory



Security depends more on what you get wrong, than what you get right!

For more information about security blunders:

RG Johnston & JS Warner,

Handbook of Security Blunders

(due out shortly)

The Top 10 Blunders

1 Lack of Critical/Creative Reviews & AVAs

2 No countermeasures for Cognitive Dissonance

3 Compliance-Based Security

4 Confusing Inventory with Security

5 Confusing Control with Security

The Top 10 Blunders

6 Thinking that finding vulnerabilities is bad news & means that somebody has been screwing up

7 Mindless faith in "Security in Depth"

8 Thinking that all vulnerabilities can be found & eliminated

9 Focusing on threats instead of vulnerabilities

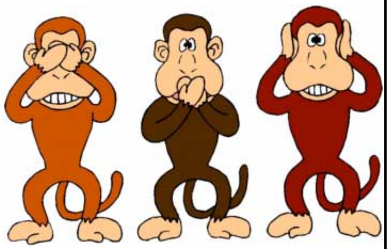
10 Mindless faith in Technology & Snake Oil

Blunder #2: No Countermeasures for Cognitive Dissonance

Cognitive Dissonance dangers:

- self-justification
  (self-serving rationalization & excuse making)
- paralysis/stagnation
  (not addressing problems)
- confirmation bias / motivated reasoning
  (interpret data only in ways that make us feel good)

> I don't want any yes-men around me. I want everyone to tell me the truth—even if it costs him his job.
> -- Samuel Goldwyn (1879-1974)



Countermeasures for Cognitive Dissonance

- appreciate how hard security really is
- avoid binary thinking
- watch out for over-confidence
- welcome input, questions, criticism, & controversy
- be your own devil’s advocate and/or appoint one
- avoid groupthink
- be uncomfortable/scared
- embrace appropriate humor

Snake Oil: Polygraphs

National Academy of Sciences $860,000 study:
“The Polygraph and Lie Detection” (October 2002)
http://www.nap.edu/books/0309084369/html/

Some Conclusions:

“Polygraph test accuracy may be degraded by countermeasures…”

“…overconfidence in the polygraph—a belief in its accuracy that goes beyond what is justified by the evidence—…presents a danger to national security…”

“Its accuracy in distinguishing actual or potential security violators from innocent test takers is insufficient to justify reliance on its use in employee security screening…”

Example of Blunder #10:
Unwarranted Confidence in **Data Encryption/Authentication**

- Intended for public communication between two secure points in space or time.

- Provides reliable security <u>if and only if</u> the sender and the receiver are physically secure, the insider threat has been mitigated, and there's a secure cradle-to-grave chain of custody on the hardware and software. (Usually none of these are true!)

- Encryption or Data Authentication techniques do not guarantee the veracity of data that is...
  - wrong
  - gathered using devices designed, constructed, operated, & controlled by people you can't trust.

> The security of a cipher lies less with the cleverness of the inventor than with the stupidity of the men who are using it.
> -- Waldemar Werther

Other Common Blunders

- VIPs bypass security
- Overly complex, changing, variably interpreted, stupid security rules
- Security rules that only the good guys follow
- Security Theater

Other Common Blunders

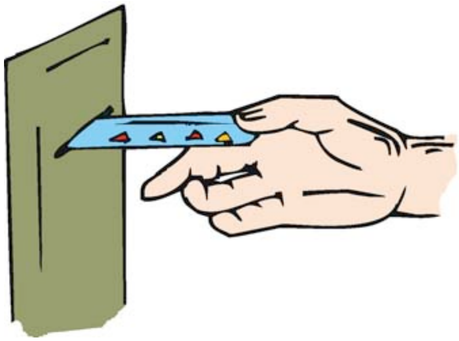
- Mindlessly banning new technology instead of intelligently accommodating it
- Too focused on prevention (which is difficult), not enough on mitigation & resiliency
- Thinking that chain link fence with barb wire represents a significant obstacle
- Over-classifying information: If everything is sensitive or classified, then nothing is!

Other Common Blunders

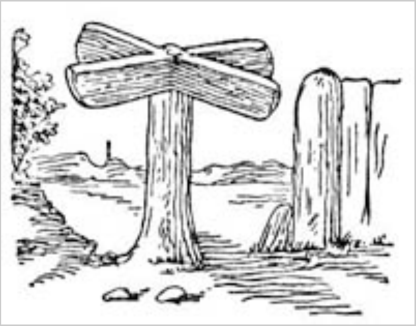
- Too much emphasis on protecting physical assets
- Not adequately protecting PII
- No (or poor) 2-person rule
- Poor quality video surveillance
- Security by Obscurity—see Shannon’s (Kerckhoffs’) Maxim!
- Not factoring in screw ups—see Rohrbach’s Maxim!

Access Control (AC) Blunders

- No role-based access; Not changing access with promotions & personnel changes
- Guards don't know what an attack looks like
- Not protecting AC devices cradle-to-grave
- No significant tamper detection



Access Control (AC) Blunders (con't)



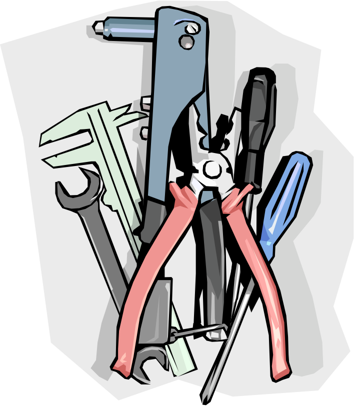
- Bad door or turnstile design
- Not tracking who exits
- Not securing the equipment and personnel that make ID badges
- Not inspecting or testing AC devices properly

"Badges? We don't need no stinkin' badges!"
-- From the movie *The Treasure of the Sierra Madre (1948)*
[The actual dialog was, "Badges? We ain't got no badges. We don't need no badges! I don't have to show you any stinkin' badges!"]

Access Control (AC)

For most AC systems, it's easy to tamper with:

- power
- software
- hardware
- database
- microprocessor
- communications
- backdoor attacks
- door lock or turnstile

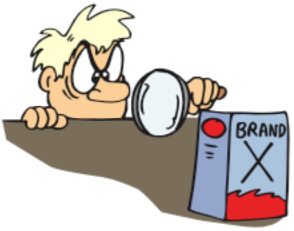


I do not care to belong to a club that accepts people like me as members.
-- Groucho Marx (1890-1977)

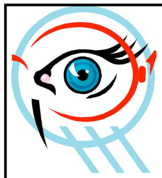
Access Control (AC)

Question: Is that really your AC device, or is it a counterfeit or a tampered version?
(…perhaps one that lets anybody in, with occasional random false rejects to look realistic.)

- Maintain a secure chain of custody, right from the factory.
- Check at random, unpredictable times with random, unpredictable people that the unauthorized are rejected.



I was the kid next door's imaginary friend.
-- Emo Philips



Biometrics Blunders

All the blunders of access control, plus:

- Not understanding how easy it is to counterfeit a biometric signature
- Downloading the entire database to satellite stations
- Not turning off the enroll function on satellite stations
- Believing the snake oil & bogus performance specs

> I'm always amazed to hear of accident victims being identified by their dental records. If they don't know who you are, how do they know who your dentist is? -- Paul Merton

Common Cargo Blunders

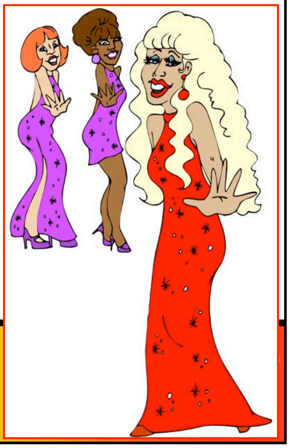
- Allowing private vehicles in loading dock areas
- Trucks are not prohibited from stopping the first 150 miles from the departure point
- Not realizing that drivers are involved in 80% of all truck cargo thefts
- Chaotic staging and loading dock areas
- Not having separate, secure, enclosed storage areas for high-value cargo

Common Cargo Blunders

- Truck drivers are allowed in the loading dock area
- Not parking loaded trucks back to back overnight if the parking area lacks good security measures
- Not having perimeter security patrols at unpredictable times
- Not painting identification numbers on the top of trucks and transportainers so they can be spotted from the air during emergencies

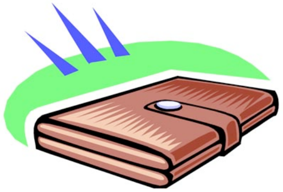
Common Cyber Blunders

- ➢ Using PCs instead of Macs
- ➢ Not realizing that Macs can pass along PC malware (and aren’t totally immune themselves)
- ➢ Not keeping malware-checking software up to date
- ➢ Not preparing employees for the “CD on the desk” & the “thumb drive in the parking lot” problems
- ➢ Not doing regular backups



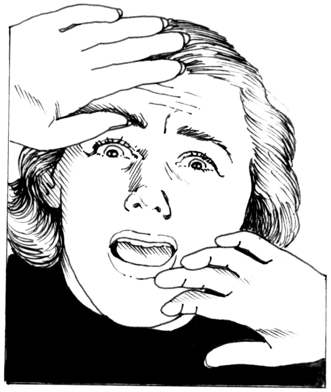
Common Cyber Blunders

- Not physically protecting computers, peripherals, & data storage
- Not appreciating the ease & speed with which an internal hard drive can be removed and copied
- Not warning employees of the security hazards (business & personal) of social networking sites (Facebook, MySpace, LiveJournal, LinkedIn, etc.)
- Not letting employees keep a copy of their passwords in their wallet



Common Cyber Blunders

- Not encouraging employees to turn off wifi and their computer, and close/reset web browsers when not in use
- Not informing employees that a land-line phone call is more secure than email
- Thinking that Open Source software is less secure than Closed Source
- Not constantly warning employees about scareware

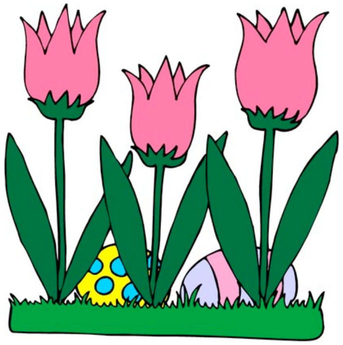


Common Cyber Blunders

- Not having the computer lock up after 30-60 mins of non-use

- Not understanding all the ways that MicroSoft Word, PowerPoint, Excel, and Adobe Acrobat (.pdf) files can sneak information—either inadvertently or deliberately—out of your organization

"How long is this Beta guy going to keep testing our stuff?"
-- Actual inquiry from a senior manager



Blunder: Hidden MS Office & .pdf Information

Some of the mechanisms:

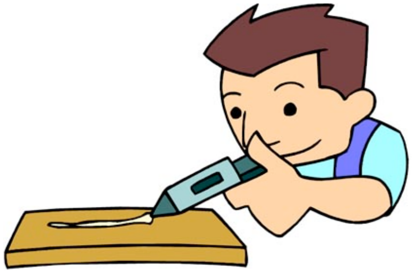
- Emailing files using Outlook automatically turns on Ad Hoc Review (change tracking), though it is often on anyway.
- Meta Data
- Invisible headers, footers, footnotes, & endnotes
- Notes/Comments, including embedded comments
- Cropped images
- Images or text fields outside the viewable area
- Drawing Objects that look like images but have grouped, hidden data
- Embedded objects
- White text on white background
- ”Alternate text" field for web posting
- Tables of height zero aren’t visible
- Orphaned objects that don’t show up
- Data that appears to be redacted (blacked out) in a pdf file but isn’t
- A key stroke tracker option that’s easy to inadvertently turn on
- Pasting a Chart also pastes the spreadsheet data, not just the graphic!

Blunder: Hidden MS Office & .pdf Information

Countermeasures:

- Start each document out as fresh blank document, rather than starting from a pre-existing document

- Turn off Ad Hoc Review



- Use "Paste Special" not "Paste"

- Rigorous review of each document

- Sanitize and redact documents before porting to .pdf form, instead of editing the pdf files

Not good solutions: text searches, Meta Data cleaners

Blunder: Poor Insider Threat Countermeasures

- Research has shown that employee disgruntlement is a risk factor for workplace violence, sabotage, theft, espionage, and employee turnover (which is not good for security).

- While disgruntlement is certainly not the only insider threat issue, it is an important one.

Blunder: Poor Insider Threat Countermeasures

- Phony or non-existent grievance & complaint resolution processes (Note: if good, they'll be used a lot)

- Phony or non-existent anonymous whistle blower program & anonymous tip hot line

- No constraints on bully bosses or HR tyranny

- Emphasis on being "fair" instead of treating EVERYBODY well

Employee perceptions are the only reality!

Wow…if only a face could talk!
-- Sportscaster John Madden
during Super Bowl coverage

Blunder: Poor Insider Threat Countermeasures

- Not managing expectations
- Not being prepared for domestic violence coming into the workplace
- Not watching for the usual precursors to insider attacks due to disgruntlement, especially sudden changes in:
  - use of drugs or alcohol
  - signs of aggression or hostility
  - not getting along with co-workers
  - performance levels
  - being late for work or no show

Blunder: Poor Insider Threat Countermeasures

- Insufficient, non-periodic background checks
- Not testing if your employees can be bribed
- Thinking that only your employees are insiders
- Thinking that low-level employees are not a major threat
- No employee assistance program, or the employees are afraid to use it
- Not publicly prosecuting insider offenders

Blunder: Poor Insider Threat Countermeasures

- Not educating employees about standard espionage risks
  - industry "surveys"
  - headhunters & CVs
  - trade secrets subtly sought at conferences, trade shows & hospitality suites
  - bars & restaurants near the facility
  - when employees are foreign nationals

Blunder: Thinking Engineers Understand Security

Engineers...

- ...make things work but aren't trained or mentally inclined to figure out how to make things break

- ...tend to think technologies fail randomly, not by deliberate, intelligent, malicious intent

- ...are not typically predisposed to think like bad guys

- ...focus on making things easy for the user—not difficult for the bad guys

- ...like products to be simple to maintain and repair—which usually makes it easy to attack

Security Device Design Blunders

- Failing to disable or eliminate diagnostics and backdoors used during development
- Worrying about high-tech attacks. (It’s a waste of time, the low-tech ones will work just fine!)
- Slapping new technology onto a device without careful thinking
- Having poor controls for hardware and software changes

Security Device Design Blunders

- Not including photos of the design in the user’s manual so end-users can check for tampering and foreign components
- Having an overly complicated enclosure
- Providing easy access to the interior, especially the microprocessor and memory
- Leaving lots of empty space inside. (Better to use baffles or clear potting compound instead.)

Security Device Design Blunders

- Lacking tamper-indicating enclosures or cases
- Lacking no tamper detection, or only a mechanical tamper switch (about the same as no tamper detection)
- Not having the sensors watch each other or the microprocessor
- Using sockets for key electronic components
- Not using ball grid IC's

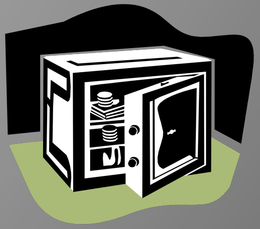
Inventory vs. Security

Inventory

- Counting and locating stuff
- No nefarious adversary
- May detect innocent errors by insiders, but not surreptitious attacks by insiders or outsiders.

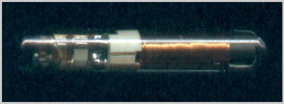
Security

- Meant to counter nefarious adversaries (insiders and outsiders)
- Watch out for mission creep: inventory systems that come to be viewed as security systems!



Examples of confusing Inventory & Security, High-Tech & High-Security

- rf transponders (RFIDs)

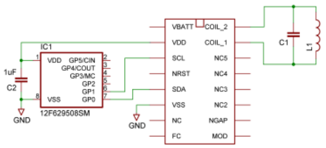


- contact memory buttons

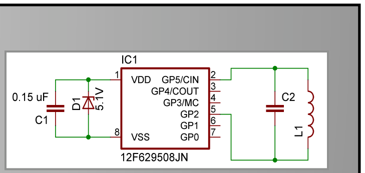
- GPS

Usually easy to:
* lift
* counterfeit
* spoof the reader

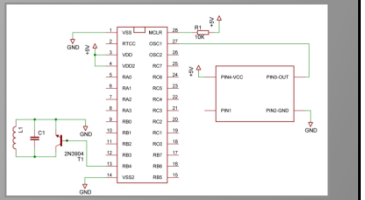
Very easy to spoof, not just jam!



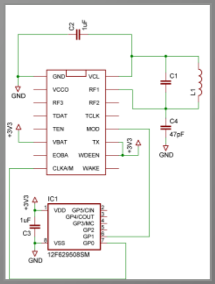
A few RFID attacks



- Communication Based:
  - Skimming: reading data off of someone else's transponder without their knowledge with a reader (home built or commercial).
  - Sniffing: “listening in” to a tag/reader communication stream.
  - Denial of Service: DoS prevents communication from occurring.
  - Spoof tag/reader communication: The act of sending a false (but correctly formatted) communication stream to the tag or reader.
  - Replay Attack: Recording data off one tag and playing it back later.



- Tag Based:
  - Clone: impersonate a tag (legitimate/home built) with stolen data.
  - Reprogramming: change data on a tag, works on select tags.
  - Tracking: Track a user or users habits using RFID data on their person.
  - Virus and Worm Injection: Use RFID tag as a carrier for a computer virus.
  - Tag Destruction: Destroy tag so that it cannot communicate.



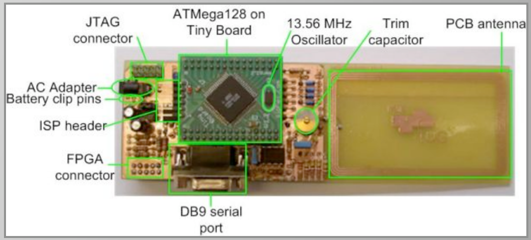
- Reader Based:
  - Reader Modification: attack the reader electronics.
  - Man-In-The-Middle/Manipulate-In-The-Middle: Intercept data

A Sampling of RFID Hobbyist Attack Kits Available on the Internet

Commercial: $20 Car RFID Clone (Walmart)

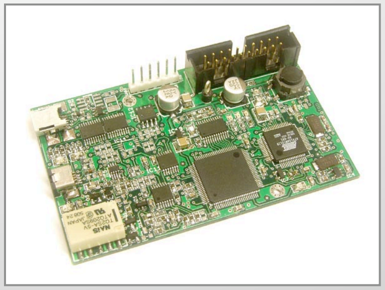
autobahn™
Universal Car Alarm
Remote Control
Quick Duplicator
Don't get stranded with a broken or lost car alarm remote.
• Create a spare in only 3 seconds
• Can be used as a garage door and gate opener
• Automatic duplication with nothing to program
• Compatible with all worldwide makes and models
• Replace lost or damaged car alarm remotes
• Works with all button functions - remote engine starters, alarms, door locks, etc.
• Create a spare back up for emergencies
• Quick and easy set up
• Durable long life ABS case
autobahn™

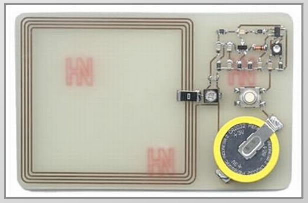
Commercial: Used for "faking RFID tags", "reader development."

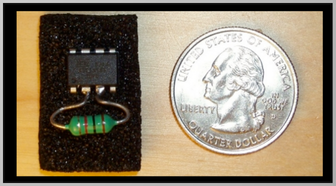


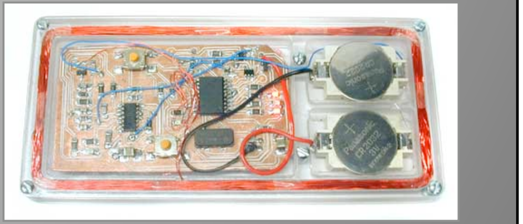
RFID Skimmers, Sniffers, Spoofers, and Cloners; oh my!

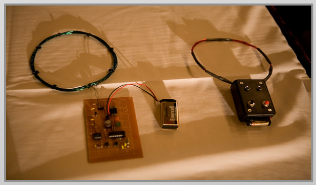
Documents, code, plans needed to build your own: free.

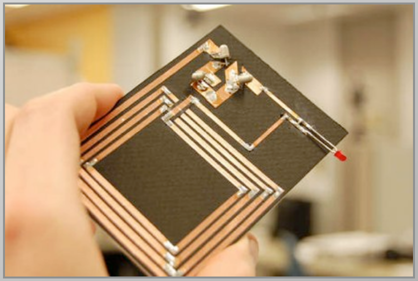


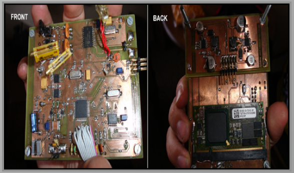




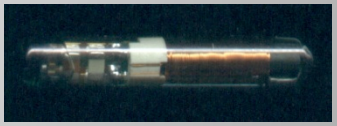








Optical Bar Code vs. RFID



RFID:

- Typically easier to “lift” than the paper barcode
- Easier to spoof the reader at a distance
- Non-visible so harder for the user to spot attacks
- Flakier → less secure

RFID is even less secure than paper bar codes!

GPS: Not a Security Technology

- The private sector, foreigners, and 90+% of the federal government must use the civilian GPS satellite signals.

- These are unencrypted and unauthenticated.

- They were never meant for critical or security applications, yet GPS is being used that way!

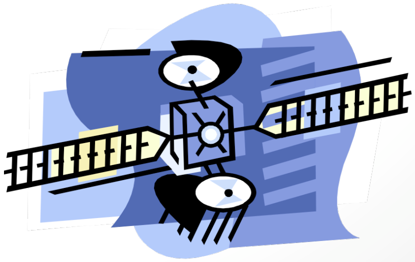
- GPS signals can be: Blocked, Jammed, or Spoofed

Spoofing Civilian GPS Receivers

- Easy to do with widely available GPS satellite simulators.
- These can be purchased, rented, or stolen.
- Not export controlled.
- Many are surprisingly user friendly. Little expertise is needed in electronics, computers, or GPS to use them.

GPS Cargo Tracking

GPS Satellite



GPS Signal

(vulnerable here)

Tracking Information Sent to HQ
(perhaps encrypted/authenticated)

GPS is great for navigation, but it does not provide security.

If a GPS tracker tells you the truck is off course do you ignore the data? (No!)

If a GPS tracker tells you the truck is on course do you bet your career on it? (No!)

Some Potential GPS Spoofing Attacks

- Crash national utility, financial, telecommunications & computer networks that rely on GPS for critical time synchronization
- Steal cargo or nuclear material being tracked by GPS
- Install false time stamps in security videos or financial transactions
- Send emergency response vehicles to the wrong location after an attack
- Interfere with military logistics (DoD uses civilian GPS for cargo)
- Interfere with battlefield soldiers using civilian GPS (against policy, but common practice anyway)
- Spoof GPS ankle bracelets used by courts and GPS data loggers used for counter-intelligence
- The creativity of the adversary is the only limitation

The Good News: Low-Cost Countermeasures

Look (in hardware or software) for artificial characteristics of GPS satellite simulator signals (or pre-recorded real GPS signals):

- Check the time intervals
- Monitor relative signal strength
- Monitor absolute signal strength
- Do a time comparison “Sanity Check”
- Perform a motion-based “Sanity Check”
- Monitor # of satellites & ID codes received
- Monitor signal strength of each received satellite

None of these countermeasures are currently in use. They would require about ~$15 in parts (retail).

Inventory vs. Security Misconceptions

- An inventory system spots missing items, therefore it detects theft.

Wrong!

- I can just add security to my existing inventory system.

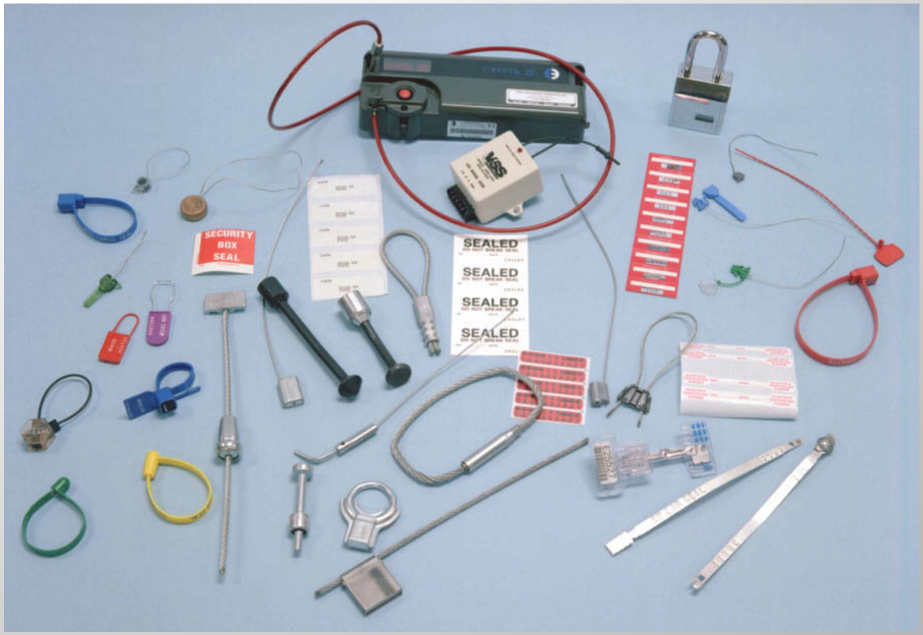
This almost never works well.

- Bad guys don’t really want to cover their tracks.

We disagree.

Seals

Seals: Detect tampering
& unauthorized access

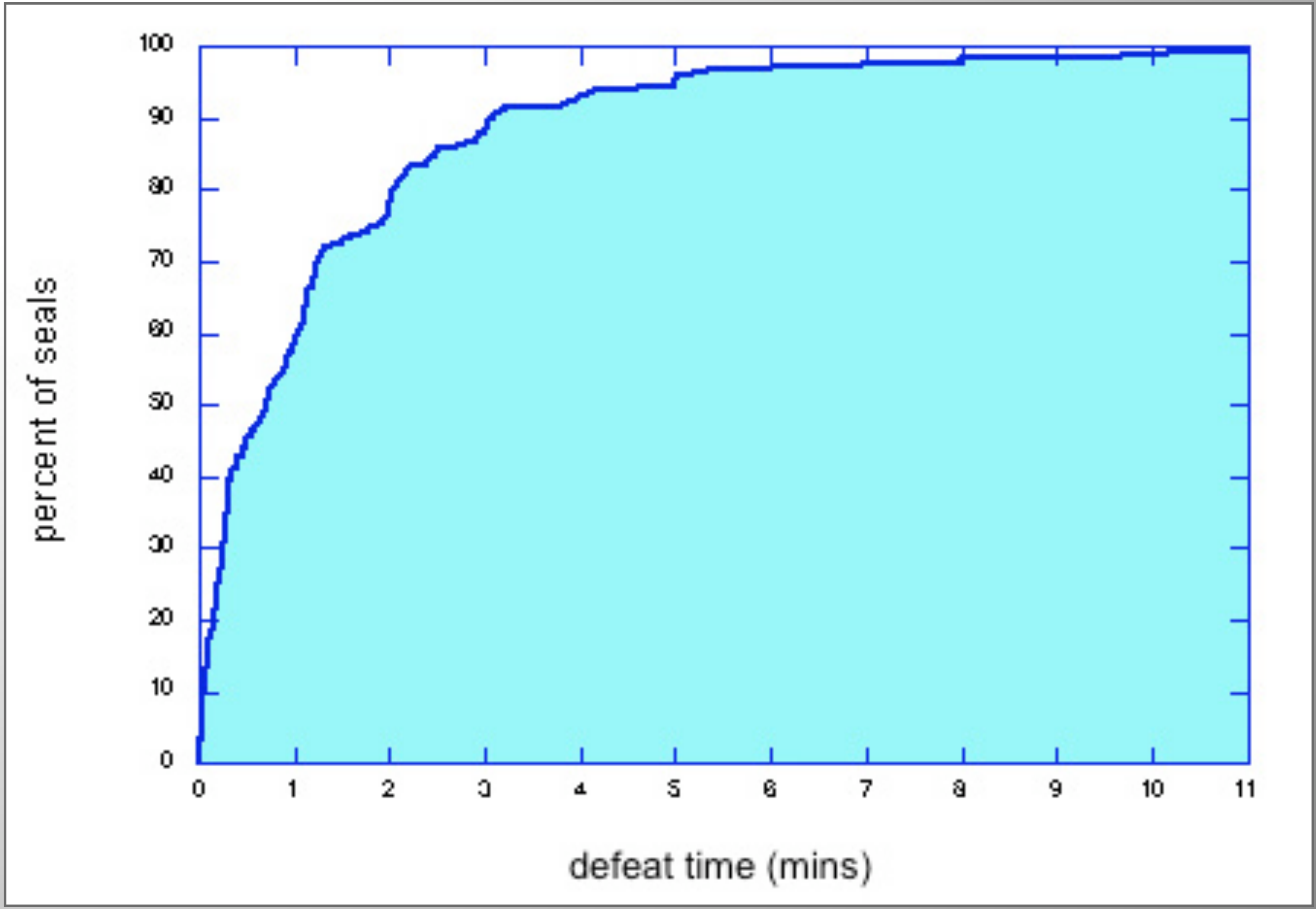


Some of the 5000+ commercial seals

Applications

- customs
- cargo security
- counter-terrorism
- counter-espionage
- banking & couriers
- drug accountability
- records & ballot integrity
- nuclear non-proliferation
- evidence chain of custody
- weapons & ammo security
- tamper-evident packaging
- anti-product counterfeiting
- protecting medical sterilization
- protecting instrument calibration
- waste management & hazardous materials accountability

Seals are easy to defeat: Percent of seals that can be defeated in less than a given amount of time by 1 person using only low-tech methods



244 different kinds of seals

The Good News: Countermeasures

- Most of the seal attacks have simple and inexpensive countermeasures, but the seal installers & inspectors must understand the seal vulnerabilities, look for likely attacks, & have hands-on training.

- Also: better seals are possible!

Tamper-Indicating Seal Blunders

- No hands-on training for seal installers & inspectors, including showing them attacks
- Not understanding what a seal is
- Thinking there are “tamper-proof” seals
- Thinking that tamper-evident packaging is effective
- Thinking pressure-sensitive adhesive label seals provide effective tamper detection

Tamper-Indicating Seal Blunders

- Not having effective seal use protocols
- No cradle-to-grave seal security
- Letting the truck driver remove the seal or control the seal paperwork
- Not inspecting the container and door hardware before & after use

Tamper-Indicating Seal Blunders

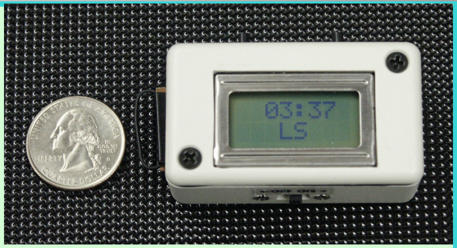
- Not saving seals for possible later forensic analysis
- Not thoroughly & securely destroying seals after use
- Locking or sealing the truck or transportainer handle, not the door
- Concentrating only on the right hand door of a transportainer

Anti-Evidence Seals

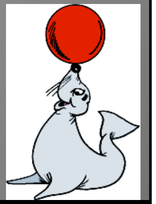
Conventional Seal: Stores the evidence of tampering until the seal can be inspected. But this ‘alarm condition’ is easy to erase or hide (or a fresh seal can be counterfeited).

Anti-Evidence Seal: When the seal is first installed, we store secret information that tampering hasn’t been detected. This is deleted when the seal is opened. There’s nothing to erase, hide, or counterfeit.

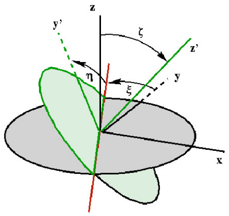
20+ New “Anti-Evidence” Seals



- better security
- no hasp required
- no tools to install or remove seal
- no hardware outside the container
- 100% reusable, even if mechanical
- can monitor volumes or areas, not just portals
- can automatically verify the seal inspector actually checked the seal (“anti-gundecking”)



Adversarial Vulnerability Assessments



- Perform a mental coordinate transformation and pretend to be the bad guys. (This is much harder than you might think.)

> It is sometimes expedient to forget who we are. -- Publilius Syrus (~42 BC)

- Be much more creative than the adversaries. They need only stumble upon 1 vulnerability, the good guys have to worry about all of them.

> It's really kinda cool to just be really creative and create something really cool. -- Britney Spears

Adversarial Vulnerability Assessments

- Don’t let the good guys & the existing security infrastructure and tactics define the problem.

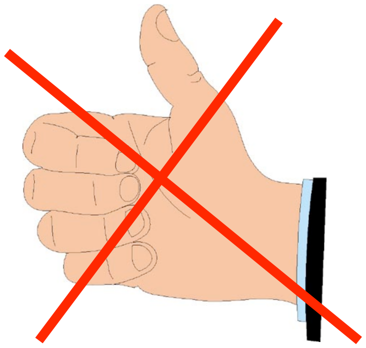
Evil will always triumph because good is dumb.
-- Rick Moranis, as Dark Helmet in *Spaceballs* (1987)

- Gleefully look for trouble, rather than seeking to reassure yourself that everything is fine.

On a laser printer cartridge: “Warning. Do not eat toner.”

Blunder: Not Understanding What a VA is for

The purpose of a vulnerability assessment is to improve security, not to:



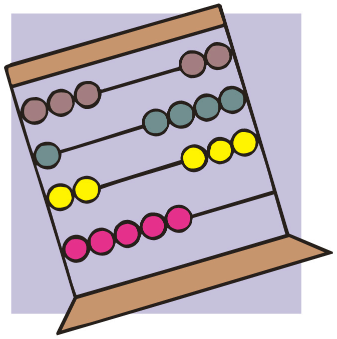
- Pass a test
- Generate metrics
- Justify the status quo
- Check against some standard
- Claim there are no vulnerabilities
- Rationalize the research & development
- Endorse a security product, or Certify it as "good" or "ready for use"
- Perform material, environmental, or quality tests
- Apply a mindless, bureaucratic stamp of approval
- Praise or accuse the developer, manufacturer, vendor, or user

Blunder: Not Understanding What a VA is for

You do NOT “pass” or “fail”
a vulnerability assessment
(or Design Basis Threat)!

Vulnerability Assessment Blunders

- Not doing vulnerability assessments (VAs) early in the design process for a new security device, system, or program—when changes are still possible and psychologically acceptable
- Not doing VA's iteratively & periodically
- Sham Rigor & the Fallacy of Precision
- Relying mostly on software tools



Vulnerability Assessment Blunders (con't)

- Relying solely on tools that don't help you find new vulnerabilities (security surveys, CARVER, DBT, etc.)
- Letting attack methods define the vulnerabilities, not the other way around
- Not using people who are creative and good at VAs (hacker mentality)
- Not using people who are psychologically predisposed to finding problems & suggesting practical fixes

Vulnerability Assessment Blunders (con't)

- Modular VAs or other artificial constraints on the VA
- Using only security experts
- Not thinking like the bad guys
- Not letting the bad guys define the problem

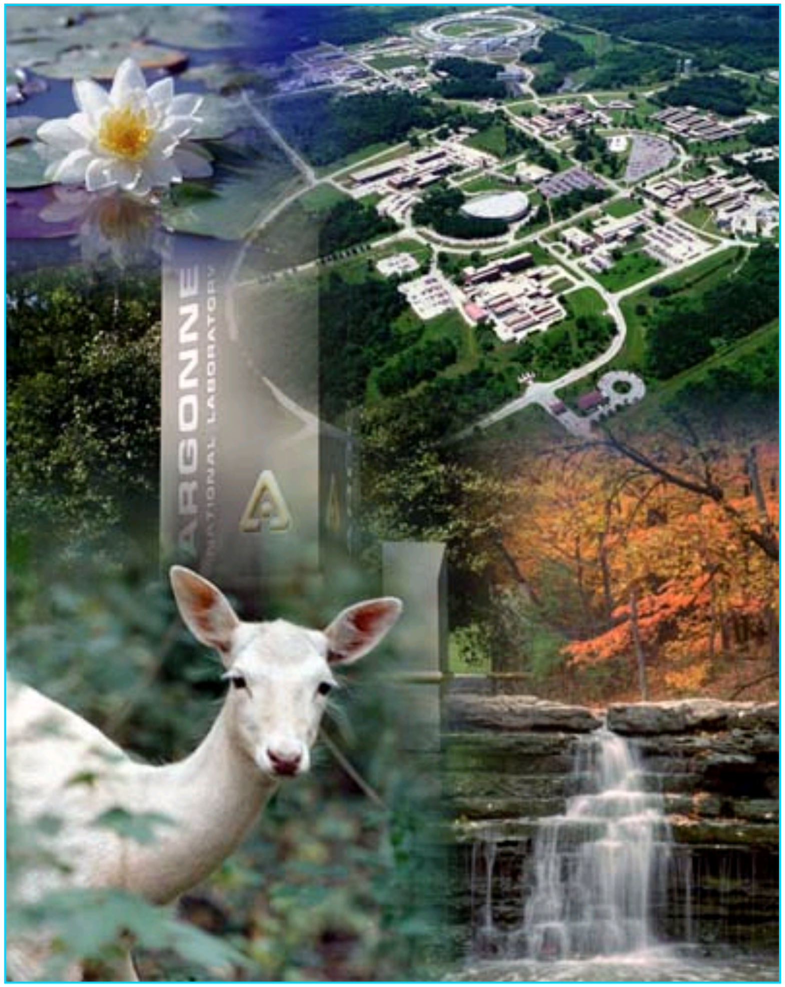
> My definition of an expert in any field is a person who knows enough about what's really going on to be scared.
>
> -- P.J. Plauger

How to Think About Thinking About Security

Whatever approaches we use, we must:

- run scared
- seek multiple inputs
- welcome controversy, criticism, & questions
- be creative & flexible
- be skeptical
- engage everybody
- think like the bad guys
- avoid scapegoating & shooting the messenger
- actively guard against the dangers of cognitive dissonance

For More Information



http://www.ne.anl.gov/capabilities/vat

Related papers, reports, and presentations are available today on CD or from rogerj@anl.gov

If you look for truth, you may find comfort in the end; if you look for comfort you will get neither truth nor comfort…only soft soap and wishful thinking to begin, and in the end, despair. -- C.S. Lewis (1898-1963)

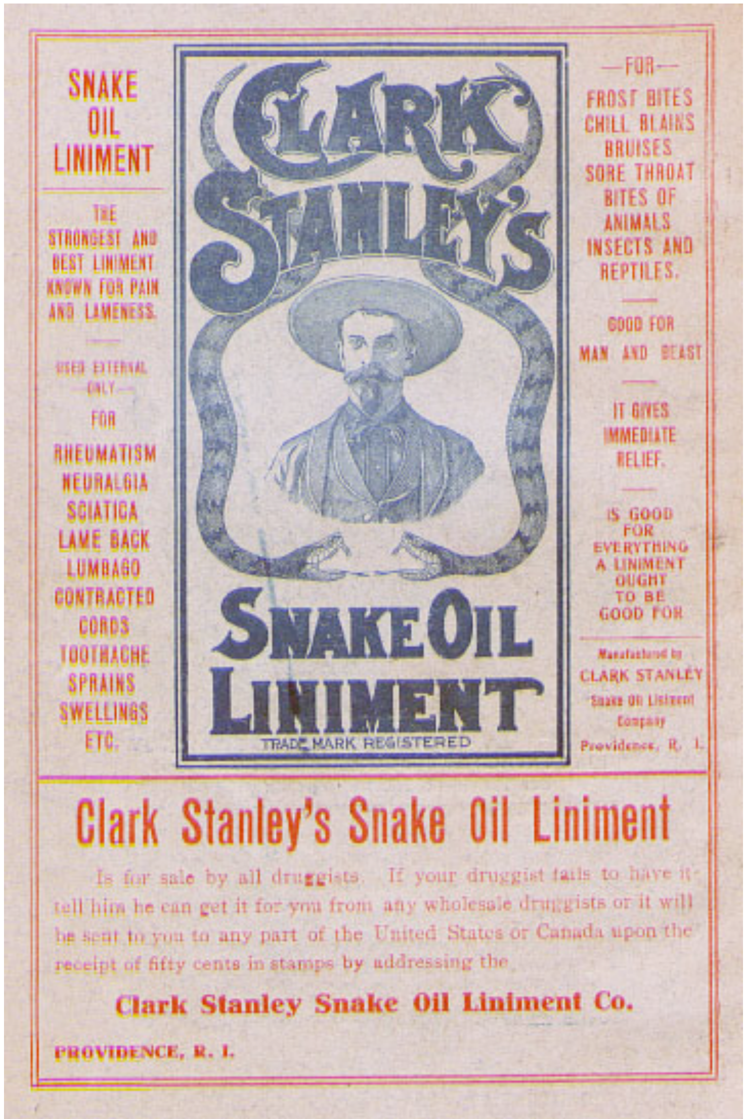
Supplemental Material

The VAT works in the following areas:

- specialty field tools
- consulting & training
- physical security R&D
- insider threat mitigation
- vulnerability assessments
- access control & biometrics
- microprocessor applications
- tamper & intrusion detection
- novel security devices/strategies
- tags & seals
- reverse engineering
- drug testing security
- electronic vote tampering
- security countermeasures
- cargo & transportation security
- security culture & human factors
- product tampering & counterfeiting
- nuclear safeguards/nonproliferation

> Rat complaints have gone up, but we look at that as a positive thing, because more people know how to contact us now.
>
> -- New York City pest control bureaucrat

Origins of the Term “Snake Oil”



SNAKE OIL LINIMENT

THE STRONGEST AND BEST LINIMENT KNOWN FOR PAIN AND LAMENESS.

USED EXTERNAL —ONLY—

FOR

RHEUMATISM
NEURALGIA
SCIATICA
LAME BACK
LUMBAGO
CONTRACTED CORDS
TOOTHACHE
SPRAINS
SWELLINGS
ETC.

CLARK STANLEY'S SNAKE OIL LINIMENT

TRADE MARK REGISTERED

—FOR—

FROST BITES
CHILL BLAINS
BRUISES
SORE THROAT
BITES OF ANIMALS
INSECTS AND REPTILES.

GOOD FOR MAN AND BEAST

IT GIVES IMMEDIATE RELIEF.

IS GOOD FOR EVERYTHING A LINIMENT OUGHT TO BE GOOD FOR

Manufactured by
CLARK STANLEY
Snake Oil Liniment
Company
Providence, R. I.

Clark Stanley’s Snake Oil Liniment

Is for sale by all druggists. If your druggist fails to have it tell him he can get it for you from any wholesale druggists or it will be sent to you to any part of the United States or Canada upon the receipt of fifty cents in stamps by addressing the

Clark Stanley Snake Oil Liniment Co.

PROVIDENCE, R. I.

Ancient World: medicines made from snakes are believed to have curative powers.

1880: John Greer’s snake oil cure-all.

1893: Clark Stanley (“The Rattlesnake King”) sells his Snake Oil Liniment at the World’s Columbian Exhibition in Chicago. A big hit. Turned out to contain no snake extract, but rather mineral oil, camphor, turpentine, beef fat, and chile powder.

Today: A product is called “snake oil” if it is fake, shoddy, or severely over-hyped.

Blunder: Mindless Faith in Technology

- **Encryption/Data Authentication**: not silver bullets
- **Biometrics**: currently easy to spoof
- **Other Access Control** : currently easy to spoof
- **Locks** : often very easy to defeat
- **Seals** : currently easy to spoof
- **Polygraphs** : pseudo-scientific nonsense
- **Product Anti-Counterfeiting Tags** : easy to counterfeit

Blunder: Not Appreciating the Broken Window Theory

All of these should look sharp, clean, professional, and well-maintained:

- guards
- reception area
- parking lot
- fence line
- loading dock
- trucks & transportainers
- general facility

Blunder: Wrong Assumptions about Counterfeiting

- Usually much easier than developers, vendors, & manufacturers claim.

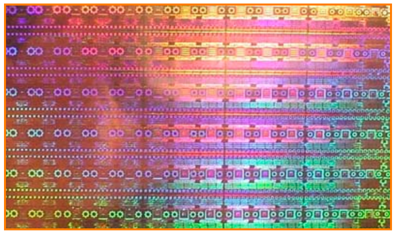
- Often overlooked: The bad guys usually only needed to mimic only the superficial appearance of the original and (maybe) counterfeit the apparent performance of the product or the security device, not the thing itself, or its real performance.

Sincerity is everything. If you can fake that, you've got it made.

-- George Burns (1885-1996)

Definition

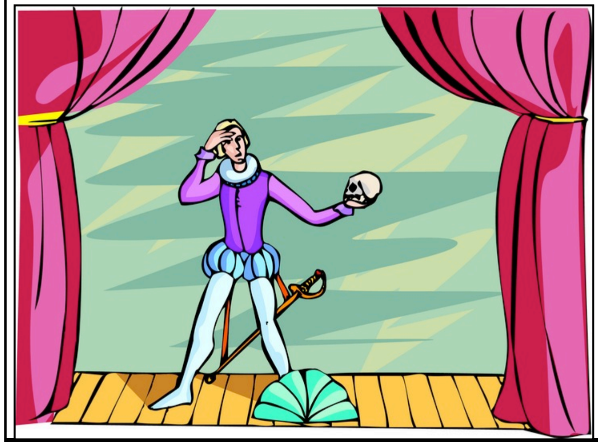
Product Anti-Counterfeiting Tag: (noun)-Something that product manufacturers and counterfeiters place on a product to convince the customer that it is authentic.



It is estimated that only 1% of "Louis Vitton" designer purses are authentic.

Good AVAs Require

1. skepticism (or cynicism)
2. creativity/imagination
3. confidence (or swagger/smirking)
4. role playing (or method acting)



We need to be more like <u>fault finders</u>. They find problems because they want to find problems, and because they are skeptical:

- bad guys
- therapists
- movie critics
- computer hackers
- scientific peer reviewers
- mothers-in-law

I told my psychiatrist that everyone hates me. He said I was being ridiculous--everyone hasn't met me yet.
-- Rodney Dangerfield (1921-1997)

"Two mothers-in-law."
-- Lord John Russell (1832-1900), on being asked what he would consider proper punishment for bigamy.

Vulnerability Assessment Blunders

Not considering all these kinds of attacks:

false alarming
power analysis
fault analysis
buffer overflow
divide by zero
time slip
saturation
counterfeiting
man-in-the-middle
SOH attacks
wait & pounce
poke the system
backdoor attacks

thermal attacks
solvent attacks
side channel attacks
picking attacks
social engineering
impersonation
espionage
sabotage
product tampering
tampering with user's manual
tampering with security training
insider, outsider, & insiders with outsiders attacks

Common Personal Security Blunders

- Not having your car key ready to go when going into the parking lot
- Not paying attention to your surroundings
- Not walking deliberately
- Not changing entry keys when you move to a new home
- Not having cash readily available should you be mugged

Common Personal Security Blunders

- Not making use of parking lot escort personnel
- Failing to practice dialing 911 on your cell phone without looking
- Not paying attention to what the sales clerk is doing with your credit card
- Not securing 2nd story windows
- Not locking doors, windows, your car, and your garage when you are home

Common Personal Security Blunders

- When on travel, not checking with locals on high crime areas
- In a hotel, not checking that windows, sliding doors, and intra-room doors are locked
- Not proceeding to the boarding area of the airport as soon as possible (the most secure spot)
- Not thoroughly checking out charities you donate to

Common Personal Security Blunders

- Leaving keys, a garage door opener, or personal information in your car when turning it over to valets

Nobody goes to that restaurant anymore because it is always so crowded.
-- Yogi Berra