

**M**ost of us are suckered at some point in our lives: coaxed, threatened, heart-strung, or baited into doing something against our better judgment. After it happens, we often feel foolish; although, in truth, falling for a con is seldom a question of intelligence. As humans, we are bound by both nature and nurture to the social contract—which, like many contracts, might be twisted to our disadvantage.

Such twisting is called “social engineering.” In a business context, a thief (“social engineer”) finds a target and exploits that person’s compulsion to be liked, to avoid confrontation, or to prevent embarrassment. Usually the target is a gatekeeper: someone who has or can provide privileged access to physical or information assets.

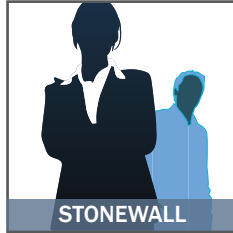
Although social engineering can be complex and clever, it’s usually simple and short-lived. You’ll be asked to break a rule. There will be extenuating circumstances. You won’t have much time to think, and the emotional pressure—typically anger, camaraderie, or desperation—will escalate quickly. Maybe there will be tears.

The key to rebuffing this sort of exploit lies less in recognizing it when it happens than in hardening yourself to it ahead of time. Being aware of your environment is your first defense. Knowing what information you may share, and when to say *no*, is another. The most critical defense, however, is understanding that it’s okay to break the social contract in the interest of security.

Company policies and procedures can also be great assets in thwarting social engineering attacks. As an authoritative reference for security practices, policies limit opportunities for dangerous judgment calls. In the event that your security judgment is challenged, policies can also offer a solid “fall back” defense. Finally, policies provide contact information for reporting security incidents after they occur. Reporting any social engineering enterprise is not only good practice, it’s a way to gain healthy validation for your difficult choices.

# How to Thwart a Social Engineering Exploit

## A REALITY-BASED GUIDE



STONEWALL

**“No” is the first,** if weakest, defense against a social engineering exploit. In some situations, it can be a flexible and effective deterrent. However, for a determined intruder, it’s an invitation to a negotiation, or a battle of wills that might eventually lead to “yes.” The other challenge in “no” is that it runs contrary to our social conditioning, that aversion to confrontation that most of us learn as children. “Nos” are strongest when you are absolutely certain that you’re right. If you recognize that you *can* be bullied, flattered, or guilted into going against your better judgment, however, you really should have a Plan B defense.



PLAY DUMB

**If knowledge is a weapon,** ignorance is armor. Your real or feigned inability to provide access authorization, a network login, the CFO’s vacation schedule, or any other sensitive information can stop would-be intruders in their tracks. The “play dumb” defense is most effective when dealing with external parties; in particular, vendors, visitors, and contractors who don’t know how smart you really are and don’t have access to your job description. Beware the rebound, however. A determined intruder might move on to seek more gullible targets. Stick with them (or enlist someone else to) and ensure they don’t make trouble.



PASS THE BLAME

**Love ‘em or loathe ‘em,** policies are great defenses against social exploits. If it were up to you, you’d do it. But, hey, *they* have rules about these things. If you can’t honestly defer to actual policies, blame the boss, a computer error, or a generic administrative assistant. Any external factor can put a firewall between a social engineer and your discretionary powers. Pleading policy can be especially effective against “authority” exploits, since even senior executives are bound by company rules. In “camaraderie” exploits, blaming “the boss” can help you turn the emotional tables on the perpetrator, since they can’t both be your pal *and* want you to get in trouble.



SECURE THE BAIT

**The next-best thing to** increasing your defensive capabilities is to decrease the value of evading them. Securing physical and electronic information can help ensure that, even if the social engineer can distract or dodge you, they will still be thwarted in their ultimate goal. Store sensitive papers and media out of site and, whenever possible, in locked offices and drawers. Don’t leave sensitive documents in public receptacles, such as trash bins, fax machines, and copiers. Ensure that computer login timeouts and timed screensavers work. And, finally, be aware that personal effects such as knickknacks and photos can fuel camaraderie and flirting exploits.

COMPILED BY T2P STAFF

[EXTRA]

## MANIPULATION TACTICS THREE APPROACHES, THREE DEFENSES



**AUTHORITY / INTIMIDATION**  
Aggression elicits a hormonal response that makes us act irrationally. Detach from the situation, respond apologetically, and call in back up—especially if the aggressor claims to be an executive or authority.



**CAMARADERIE / FLIRTING**  
Remember: it’s not personal. Blame policy to deflect requests to share information in confidence. Use your “connection” with the perp to draw out intel on them. Report as much as you can to security staff.



**HELPLESSNESS / FEAR**  
Stick to hard rules for ID and verification. Make sure the instigator is watched at all times. Do not leave sensitive resources unguarded. If you can help without breaking these rules, do so. It might be a real emergency.

# References & Resources

## SOCIAL ENGINEERING

### Social Engineering Fundamentals, Part I: Hacker Tactics

Good introduction to social engineering concepts and tactics.

<http://www.securityfocus.com/infocus/1527>

### Social Engineering Fundamentals, Part II: Combat Strategies

<http://www.securityfocus.com/infocus/1533>

An overview of managerial, operational, and technical tactics that can prevent and thwart social engineering exploits.

### Social Engineering Database

A wiki-based repository of scripts, tools, attack theories, and prevention methods.

<http://www.socialengineeringdb.org>

### SANS Institute - SANS InfoSec Reading Room - Social Engineering

A collection of white papers on social engineering mechanisms, threats, and controls.

[http://www.sans.org/reading\\_room/whitepapers/engineering/](http://www.sans.org/reading_room/whitepapers/engineering/)

### US National Cyber Alert System: Cyber Security Tip ST04-014: Avoiding Social Engineering and Phishing Attacks

Definitions and tips from US-CERT

<http://www.us-cert.gov/cas/tips/ST04-014.html>

### Why Phishing Works (PDF)

A scholarly paper reflecting experiments with phishing tactics and user responses.

[http://people.seas.harvard.edu/~rachna/papers/why\\_phishing\\_works.pdf](http://people.seas.harvard.edu/~rachna/papers/why_phishing_works.pdf)

### Getting Users to Pay Attention to Anti-Phishing Education: Evaluation of Retention and Transfer (PDF)

A scholarly paper offering insight into why people fall for social engineering ploys, even they do know better.

[http://www.ecrimeresearch.org/2007/proceedings/p70\\_kumaraguru.pdf](http://www.ecrimeresearch.org/2007/proceedings/p70_kumaraguru.pdf)

### Wetware's Intrusion Prevention Systems: Defending Against Social Engineering (PDF)

A well-rounded perspective on social engineering mechanics, threats, and responses.

[http://gabiam.com/software/users/kfc/pdf/sec11\\_a5.pdf](http://gabiam.com/software/users/kfc/pdf/sec11_a5.pdf)

### SXSW: Social Engineering: Scam Your Way Into Anything or From Anybody

Entertaining podcast with live demonstrations of social manipulation and scamming.

<http://huffduffer.com/hughgarry/3661>

### Schneier on Security: Real-World Back Doors

Interesting perspective and community insight based on a UK study of smokers, camaraderie, and security.

[http://www.schneier.com/blog/archives/2007/02/realworld\\_back.html](http://www.schneier.com/blog/archives/2007/02/realworld_back.html)

### Scare Tactics: Reacting to a Crisis Without Panic

Tips on reducing knee-jerk responses that can (be used to) open security holes.

<http://www.csoonline.com/article/219050/>

### Social Engineering in Penetration Testing

A three-part series on planning, executing, and analyzing social engineering pentests as part of an information security assessment.

<http://www.networkworld.com/newsletters/sec/2007/1029sec2.html>

## ABOUT T2P COMMUNITY-CONTRIBUTED RESEARCH

Truth to Power (T2P) is an information governance research community dedicated to helping IT, business, legal, and audit professionals improve performance and reduce risk by unlocking the potential of corporate information. As part of our mission to provide practical advice, useful perspectives, and insightful analysis, T2P champions the initiative of community members to share insight and advice for the common good.

This paper epitomizes T2P's mission. The Reality-Based Guide series was designed around an article submitted by T2P member and Core Guide Ben Tomhave. By extending the Reality-Based Guide series, T2P applauds Ben's contributions as a shining example of how information professionals can help each other to advance the field as a whole.

Additional resources by and for the information community are available at <http://www.t2pa.com>.

To learn more about contributing insight and advice to the T2P professional community, please email [editor@t2pa.com](mailto:editor@t2pa.com).