What is Social Engineering and How Does it Work
What is social engineering?

Social engineering is the art of deceiving people. It is a popular tool cybercriminals use to get their dirty hands on your money. In today’s profit-driven world, cybercriminals are no longer just after infamy, they’re after your money.

Worse than the most intrusive malware, socially engineered threats are harder to protect against. Why? Because they target you, not just your system.

The most effective way to protect yourself from these threats is to stay informed. Know what to watch out for, what to avoid, and what to be careful of.

Big news can be bad news.

Buzz-worthy events like natural disasters or highly anticipated product or service launches always catch people's attention. And those with a working system and Internet access naturally surf the web to ride the wave. Little do they know nor care about the cybercriminal traps that lie in wait for them.

**WHAT YOU SEE:** Social media posts with links to hard-to-resist videos or photos

**WHAT YOU DON'T SEE:** Cybercriminals waste no time laying traps, aka malicious sites, every time a big event hits the fan. These sites, often malware laden, can automatically wreak havoc on your system. Some redirect you to surveys or ads but none ever lead to what you were promised.

**WHAT YOU SHOULD WATCH OUT FOR:** Malicious links to fake news sites or pages

---

**BUZZ-WORTHY EVENTS CYBERCRIMINALS TOOK ADVANTAGE OF**

**NATURAL DISASTERS**

Minutes after the 3/11 tsunami in Japan occurred, fake news sites hosting FAKEAV malware infected the systems of users in search of updates.


**PRODUCT OR SERVICE LAUNCHES**

A fake iPad giveaway promo tricked victims into giving away their personal information via email.

Popular celebrities make popular targets.
Celebrity news are sure to gain the most interest than any kind of news. They cater to a much wider range of audiences, mostly fans or followers, and so get more media attention, too. In the battle for readership, media outfits often had to rely on sensationalism and exaggeration to grab the public eye. The more unbelievable the headline, the more readers flocked to read about it.

WHAT YOU SEE: Links to stories with attention-grabbing headlines that promise even more incredible and scandalous revelations when clicked

WHAT YOU DON’T SEE: Like other significant news, these links often lead to specially crafted malicious sites that take advantage of the media hype surrounding the celebrity in focus. Similar to most scams, these often contain malware or redirect victims to survey or ad sites.

WHAT YOU SHOULD WATCH OUT FOR: Unbelievable headlines with links to related videos or photos

**CELEBRITY NEWS CYBERCRIMINALS ABUSED**

**SCANDALS**
A social media post promoting a video that “just ended Justin Bieber’s career for good” redirected victims to a survey site while ending up on their own pages.


**CONTROVERSIES**
Various events related to Michael Jackson’s death lured victims to download malware in the guise of an image that spread via MSN Messenger.


**FAKE DEATHS**
A fake news site spread rumors of Jackie Chan’s death to redirect victims to a malicious site.

Keep your friends close but your enemies at bay.
Millions flock to their favorite social networking sites every day. It is therefore not surprising why social networking fraud, a form of misdirection using certain aspects of social media platforms, has become a norm.

**WHAT YOU SEE:** Posts promoting new social media features only available for limited amounts of time that come with suspicious codes that must be copied and pasted onto browser address bars or apps that must be downloaded and installed in systems

**WHAT YOU DON’T SEE:** These suspicious codes or apps usually lead to malicious pages tailored to hijack accounts, steal personal information, or spread through account infections.

**WHAT YOU SHOULD WATCH OUT FOR:** Suspicious links to feature- or app-download sites

---

**SOCIAL MEDIA SCAMS CYBERCRIMINALS HAVE TRIED**

**TIMELY THEMES**

A social media post advertising a Valentine’s Day theme instead forced victims to download and install a malicious extension for their Chrome and Firefox browsers.


**NEW FEATURES**

A fake Twitter app that supposedly monitored victims’ follower activities instead allowed bad guys to hijack their accounts.

Cybercrooks will always try to spook you into giving in.
Fear is a great motivator, even cybercriminals know that. That’s why they use threats and alarmist language to urge you to give in to their desires—reveal personal information or part with hard-earned money.

**WHAT YOU SEE:** Suspicious email disguised as urgent notifications, mostly regarding system or financial safety, that require immediate action—viewing an attachment, buying an application, or making an online payment

**WHAT YOU DON’T SEE:** These threats can be likened to bad guys holding a gun to your back to take your money and other valuables. No matter how scary their tactics are, these normally don’t inflict that much harm unless you give in.

**WHAT YOU SHOULD WATCH OUT FOR:** Scary email subjects and content asking you to do something or suffer the consequence

---

**SCARY PROPOSITIONS CYBERCRIMINALS HAVE PULLED**

**RANSOMWARE**

Russian users were threatened into paying bad guys about US$15 with fake citations for viewing inappropriate content.


**FAKEAV**

FAKEAV vendors are known for tricking their victims into buying useless applications with the use of scary system infection warnings.

Threats, like seasons, come and go.
Christmas or any other widely celebrated holiday and the “Super Bowl” or any popular sporting event will always be favorite cybercriminal baits. We can therefore always expect them to usher their coming, celebrate with the masses, and muse on what has passed every single time.

**WHAT YOU SEE:** Suspicious spam and social media posts promoting unbelievable offers in time for holidays or huge sports events

**WHAT YOU DON’T SEE:** The links embedded in these lead to tailor-made sites that either host malware or redirect to survey or ad sites but never to freebies or great offers.

**WHAT YOU SHOULD WATCH OUT FOR:** Online deals that are too good to be true

---

**SEASONS CYBERCRIMINALS RIDE ON**

**HOLIDAYS**

A Facebook scam page once offered victims a free Christmas theme plug-in, which instead allowed victims’ accounts to be hijacked for spamming purposes.


---

**SPORTS EVENTS**

“Super Bowl” fans in search of updates were instead redirected to FAKEAV-hosting sites.

Social Engineering Safety Tips
BOOKMARK TRUSTED SITES.

They say trust is gained. Treat new sites like people you meet for the first time. Just like you don’t trust everyone you meet the first time you lay eyes on them, don’t immediately trust sites you’ve only visited once.

SUSPICIOUS IS AS SUSPICIOUS GETS.

Never click suspicious links, no matter how promising their accompanying messages seem. Promises that are too good to be true are just that.

FEAR IS NOT AN OPTION.

Don’t be intimidated by threats. A lot of bad guys often rely on the element of surprise to scare you into doing something you otherwise won’t. It’s always best to ignore scare tactics outright.

SPREAD THE WORD.

Tell others about what you know. Doing so will ensure your friends and relatives’ safety. Don’t let them fall for cybercriminal traps.

PREVENTION IS ALWAYS BETTER THAN CURE.

Invest in an effective security solution that protects your system and data from all kinds of threats. Explore and utilize the built-in security features of the sites and pages you frequently visit. Some sites like Facebook even provide information on the latest threats and tips to help you safely navigate through their pages.

Read up on the latest security threats and issues in the following Trend Micro blogs:

• Fearless Web
• TrendLabs Malware Blog
• Internet Safety for Kids & Families
TREND MICRO™

Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global cloud security leader, creates a world safe for exchanging digital information with its Internet content security and threat management solutions for businesses and consumers. A pioneer in server security with over 20 years’ experience, we deliver top-ranked client, server and cloud-based security that fits our customers’ and partners’ needs, stops new threats faster, and protects data in physical, virtualized and cloud environments. Powered by the industry-leading Trend Micro™ Smart Protection Network™ cloud computing security infrastructure, our products and services stop threats where they emerge—from the Internet. They are supported by 1,000+ threat intelligence experts around the globe.

TRENDLABS™

TrendLabs is a multinational research, development, and support center with an extensive regional presence committed to 24 x 7 threat surveillance, attack prevention, and timely and seamless solutions delivery. With more than 1,000 threat experts and support engineers deployed round-the-clock in labs located around the globe, TrendLabs enables Trend Micro to continuously monitor the threat landscape across the globe; deliver real-time data to detect, to preempt, and to eliminate threats; research on and analyze technologies to combat new threats; respond in real time to targeted threats; and help customers worldwide minimize damage, reduce costs, and ensure business continuity.