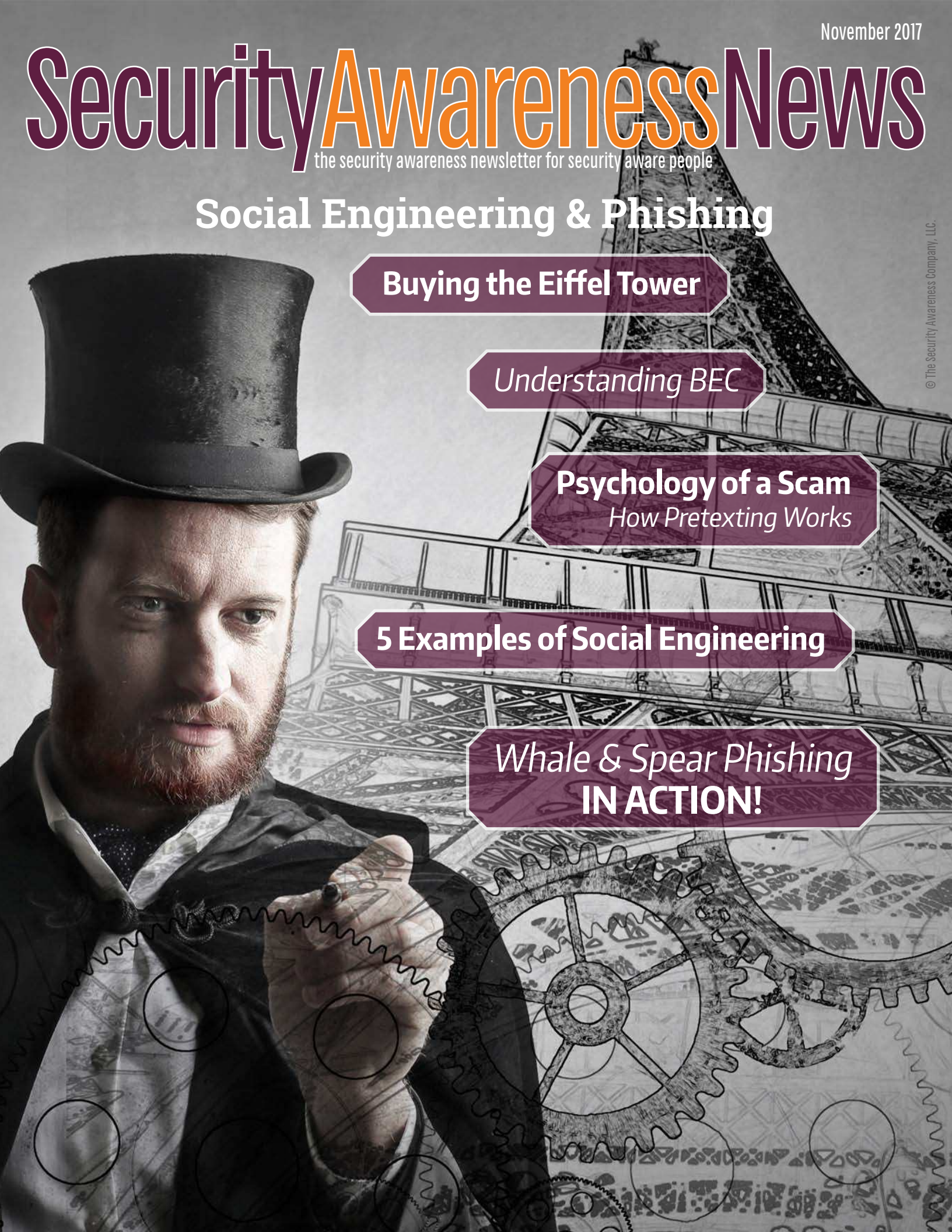
November 2017

Security Awareness News

the security awareness newsletter for security aware people

Social Engineering & Phishing



Buying the Eiffel Tower

Understanding BEC

Psychology of a Scam
How Pretexting Works

5 Examples of Social Engineering

Whale & Spear Phishing
IN ACTION!

Buying the Eiffel Tower

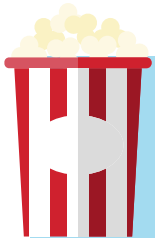
Did you know that the Eiffel Tower was not built as a permanent structure? The iconic tower was created as a part of the Exposition Universelle of 1889—a world's fair held in Paris from May to October—and was planned to be torn down and moved a few years later.

In 1925, a man by the name of Victor Lustig saw an opportunity. ***The tower had fallen into disrepair due to the cost of maintenance, so Lustig invited six metal dealers to a prestigious hotel and introduced himself as "deputy director." He told them that the city, preparing to tear the tower down, was accepting bids to buy the metal for scrap.*** One of the men, Andrew Poisson, desperate to make a name for himself in Paris, fell for the scam and paid Lustig the agreed upon bid.

Poisson was too embarrassed to go to the police after he learned he had been duped, which allowed Lustig to "sell" the Eiffel Tower, for a second time, a few years later.

It was one of many scams carried out by Lustig, who was later called the "smoothest con man that ever lived" by a Secret Service agent, and it proves that social engineers have enjoyed a long, successful history. Even today their methods haven't changed all that much. They still prey on the vulnerabilities of human emotions. ***So, while most people associate the term "hacking" with something technical that can only be done by someone with a particular set of computer skills, the truth is, most security incidents are the result of hacking humans—not computers.***

To avoid becoming a con victim, we must all stay on our toes. Never give out sensitive information about your friends, families, co-workers, our clients or our organization unless you are 100 percent sure the person on the other end can be trusted. In other words, don't buy the Eiffel Tower! ***If you discover a social engineering attack, or notice someone who doesn't belong, report it immediately.***



Social Engineers On The Big Screen
The entertainment industry is no stranger to featuring con artists in plots. Check out these social engineers in pop culture: http://secaware.co/2yiBNKG.

Other Notable Social Engineers

The Greek Army
Perhaps the original con, the Greeks breached the borders of the city of Troy via a wooden horse—presented as a gift—that concealed a small force of soldiers.

George Parker
Similar to Lustig, Parker made a living selling property he didn't own including Madison Square Garden, the Brooklyn Bridge, and the Statue of Liberty.

Charles Ponzi
Ponzi invented a scheme that promised investors they would double their money, known now as the Ponzi Scheme.

Frank Abagnale Jr.
Between the ages of 16 and 18, Abagnale impersonated pilots and flew an estimated one million miles at no charge and earned free lodging wherever he landed based on his pilot status.

Kevin Mitnick
One of the first to fuse cybercrime with social engineering, Mitnick used his skills as a con artist to gain unauthorized access to dozens of computer networks in the early 90s.

Understanding BEC

Short for **business email compromise**, BEC is one of the fastest growing scams that targets organizations. **It works like this: a cybercriminal gains access to the email address of a senior executive. They then spoof that email to send requests for money or information to employees who trust that senior executive.**

According to the FBI, BEC scams—also referred to as CEO Fraud—have cost organizations around the world $5.3 billion/€4.4 billion since 2013.[1]

In fact, according to a study conducted by Proofpoint, BEC attacks targeted nearly 85% of organizations in the first quarter of 2017 alone.[2]

What can you do about it? This is where we need everyone in our organization to play the role of Human Firewall! **Always treat requests for money or sensitive information with a high degree of skepticism. Stay alert for anything out of the ordinary, and remember there are no stupid questions. If you're not sure, please ask!**

Sources: 1. https://securityledger.com/2017/05/fbi-business-email-compromise-is-a-5-billion-industry/
2. https://www.proofpoint.com/sites/default/files/pfpt-us-ds-bec-quarterly-update.pdf

THE SOCIAL ENGINEER'S PLAYBOOK

IDENTIFY THE TARGET. Gather as much info about the target as possible (usually from data breaches that leak personal info, such as full names and email addresses).

DEVELOP A PRETEXT. A pretext is a made-up scenario used to trick victims.

ENGAGE with the target to gain trust, most often via phishing emails.

STEAL INFORMATION or finances from target.

Pretexting Definition
The practice of developing a fabricated scenario (the pretext) in order to elicit information from a target, often via phishing (emails) or vishing (phishing via phone calls/messages).

Going After Execs with CEO Fraud

Social engineers target executives and other high-ranking members of organizations via two basic phishing methods:

SPEAR PHISHING
By compromising their email addresses and sending requests for sensitive information or money transfers to lower-level employees.

WHALE PHISHING
By posing as government entities or business partners and emailing attachments of allegedly important documents which contain malware.

Good security comes from timely response. Report security incidents immediately!

Whale & Spear Phishing

The economy of cybercrime is built on access. Whether that be access to financial accounts, trade secrets, or personally identifiable information, those with the keys hold the most power, and therefore, are the most valuable targets. It makes sense that cybercriminals would go after those with the highest access. It also makes sense that those at the top seem insulated, but nothing could be farther from the truth. Whale and spear phishing campaigns are a lot more sophisticated than standard, run-of-the-mill phishing attacks, and are designed with upper management and executives in mind! Everyone is a target and everyone benefits from learning as much as they can to improve their awareness.

Whale Phishing In Action

As the name suggests, whale phishing is a social engineering attack that targets senior executives and high-profile individuals. Let's take a look an example of this, based on a real-life attack from a few years ago:

From: United States District Court (subpoena@uscourts.com)
To: Troy Smith
Subject: Subpoena in case #24-554-BDR

Issued to: Troy Smith
Acme Corporation
200-555-1000

SUBPOENA IN CIVIL CASE: Case Number: 24-554-BDR
United States District Court

YOU ARE HEREBY COMMANDED to appear and testify before the Grand Jury.

Please download the entire document on this matter and print for your record via the below link. Failure to do so will result in a contempt of court citation.

Click here to fill out document.

This whale phishing attack targeted thousands of senior executives. How could they determine that it was a scam?

For starters, government entities rarely, if ever, send official documentation like this through email. They also use ".gov" in email addresses instead of ".com".

And there's also the matter of three classic signs of phishing: threatening language, a sense of urgency, and a call to action (clicking the link).

Spear Phishing in Action

Spear phishing targets specific individuals or companies. One of the most common examples is BEC, or business email compromise. BEC attacks come in many different shapes and sizes. Here's one example:

From: jane.ceo@acmecorp.com
To: crystal.cfo@acmecorp.com
Subject: Urgent

Crystal, did you get my email from earlier? I am about to join a meeting and need this taken care of ASAP. Please process a wire of $12,550 USD to the attached wiring instructions. Let me know when the transfer is complete.

Thanks,

Jane

What's Crystal supposed to do in this situation? Her boss is asking her to take care of something important ASAP. She might not want to bother Jane if she's in a meeting. And the email itself doesn't look threatening. It comes from her boss, it uses clear language, and it addresses Crystal by name. ***What would YOU do?***

The answer is *call Jane.* Even if there's a small chance that this is a legit email, you'd be much better off interrupting a meeting, or putting off the wire transfer until Jane is available, rather than complying with the request.

As always, treat all requests for personal information or financial transfers with a heavy dose of skepticism. And report all phishing emails ASAP! If you're not sure how, please ask.

Good security comes from timely response. Report security incidents immediately!

5 EXAMPLES OF SOCIAL ENGINEERING

PHISHING

WHY IT WORKS: phishing emails prey on stoking the victim's emotional reaction with urgent or threatening language.

VISHING

WHY IT WORKS: vishing uses the exact same techniques as phishing, and sometimes is more successful because the victim is talking to a real person.

DUMPSTER DIVING

WHY IT WORKS: a lot of people wouldn't expect someone to dig through their dumpster, so sensitive information is often discarded intact.

TAILGATING

WHY IT WORKS: it's easy to be distracted on busy work days, so it's possible for an unsuspecting employee to not notice when someone slips in behind them after accessing a secure area.

PIGGYBACKING

WHY IT WORKS: people don't want to be rude so they forget about security and policy in favor of courtesy, allowing social engineers to piggyback into secure areas, both physical and cyber.

Have you ever felt an immediate and overwhelming emotional response to something? If so, then you've experienced what author and psychologist Daniel Goleman refers to as an amygdala hijack. **The amygdala is a part of the brain that is largely responsible for generating emotional responses.** When humans are presented with something that is threatening or overwhelming, the amygdala hijacks the rational brain, often leading to irrational decision making.

Social engineers love your amygdala. They set emotional traps that result in individuals overreacting to a situation, like the classic tax scam where a fraudster calls the victim and threatens them with extensive fines if payment is not made immediately. **Don't let them get to your amygdala! Use common sense, think before you click, and keep your emotions in check as best you can.**

Good security comes from timely response. Report security incidents immediately!

PSYCHOLOGY OF A SCAM
HOW PRETEXTING WORKS

BRRRING-BRRRING

Hello?

Hi. This is Donna, from IT. Is this Sam Spade in Marketing Support?

Yep!

Cool. As I said, I'm Donna from IT, and I don't know if you've noticed some funky internet behavior today...

Well, it was a little slow this morning...

We're just trying to isolate the source of the possible IP collisions, and it appears it might be coming from the intranet routing and control tables matrix over there in marketing... you follow?

Uh...sure.

Good. It should be pretty easy to find. I'm just resetting some of the accounts that look like they may have triggered the TCP or TLS runaway. I just need to reset your AD profile, in case that's where the buffer balloon begins... your email is Sam_Spade@MyCompany.com?

Correct.

And your password is...OH! Before you tell me, I need you to promise you will change it immediately, and I mean immediately, after we hang up. You know... security and all that.

I promise. OK...it's maryhad4rabbits... all lower with the number 4...

Thanks. Hold on for just a minute...

CLICK!

What did Sam do wrong? How did he know for a fact that Donna was from the IT department? Should Sam have given up his password so easily?

Pretexting can come from anyone, anywhere, at anytime. Make sure you confirm to whom you are speaking. When in doubt, get their internal number and call back. When anyone calls and asks for PII (personally identifiable information), or confidential company information, become immediately suspicious. And finally, never, ever share your password with anyone... EVER!

Good security comes from timely response. Report security incidents immediately!