SecurityAwarenessNews

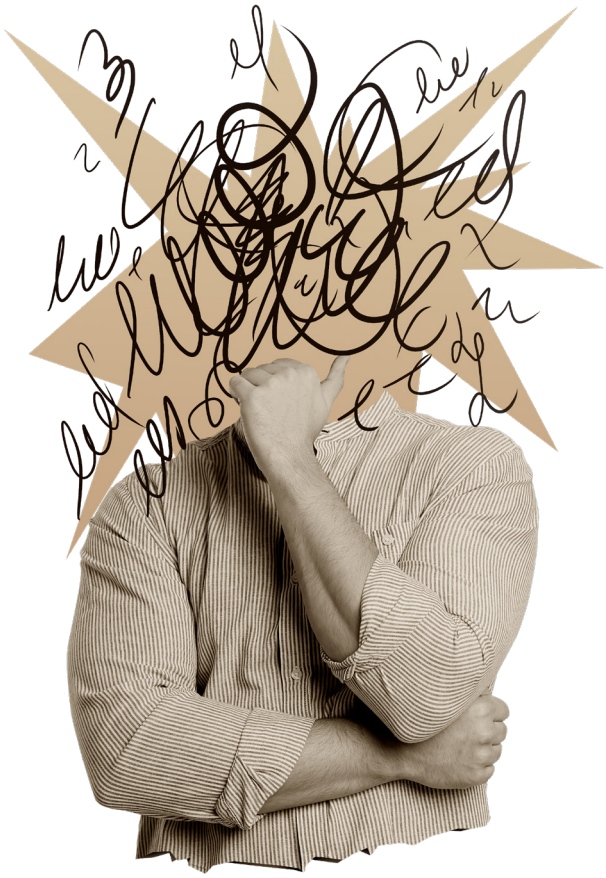
the security awareness newsletter for security aware people

Operation Influence

Phishing Identification Checklist

How Social Engineers Exploit Cognitive Biases

The Dangerous Side of Social Media



HOW SOCIAL ENGINEERS EXPLOIT COGNITIVE BIASES

Social engineering is the art of influencing people into making mistakes. Behind it lurks a calculated science of deception and psychological manipulation. Attackers leverage that science to exploit our cognitive biases — the mental shortcuts our brains use to quickly make decisions and judgments.

There are many types of cognitive biases, all of which are unfortunately subject to failure. Here are just a few examples and how social engineers use them against us.

Authority Bias

People tend to comply with requests from authority figures. Social engineers leverage this bias by impersonating managers or anyone else who might have legitimate reasons for requesting information or access.

Scarcity Bias

"For a limited time only" is a common sales technique that influences demand. This fear of missing out creates a sense of urgency, just like social engineers often do via phishing attacks and other scams.

Reciprocity Bias

People often feel an obligation to return favors. Attackers can leverage this by offering to help someone with a (nonexistent) technical problem. In return, the target might provide their password.

These examples showcase how social engineering is a blend of art and science that can lead to significant consequences. While we can't simply turn off our cognitive biases, we can implement mental countermeasures by:

Slowing down

Social engineers love catching people when they're too busy to think clearly. Hasty decisions can be costly.

Avoiding assumptions

Impersonation is one of the key tactics of attackers. Never assume someone is who they claim to be.

Always verifying

If you encounter an unusual request, reach out directly to a trusted source (such as a manager) to verify its legitimacy.

Thinking critically

Social engineers want to gain your trust and use your emotions against you. Use critical thinking before reacting.

In summary, a social engineer is an attacker who uses subtle tactics that technology alone cannot defend against. People, however, can defend against them, and it's why we will always be the last line of defense.

PHISHING IDENTIFICATION CHECKLIST

Phishing is the top attack method for social engineers. It's how they steal data, defraud people of money, and spread malicious software. Use this checklist to help identify phishing attacks:

- ☐ ***Does it push a sense of urgency?***
- ☐ ***Does it feature threatening language?***
- ☐ ***Does it offer unrealistic promises?***
- ☐ ***Does it contain suspicious links or attachments?***
- ☐ ***Does it come from a sender you don't know or didn't expect?***

If the answer is yes to one, some, or all of those questions, then there's a high likelihood you're being phished. Urgency, threatening language, and unrealistic promises are especially prevalent in phishing attacks and should immediately raise your suspicions.

On traditional computers, you can identify a malicious link by hovering your mouse over it to reveal the full URL. If it looks odd or suspicious, don't click. If you're not quite sure, don't click! For attachments, never open them unless you can be absolutely certain they're trustworthy.

Also, keep in mind that it's easy to steal real company logos or create email addresses that appear to come from a legitimate source. Always thoroughly inspect the "from" address for any alterations. For example, a domain like accounts-amazom.com has been altered to appear real (amazon is spelled incorrectly).

Putting this all together, phishing is a dangerous attack that combines manipulation and deception. By slowing down and staying alert for warning signs, you can avoid getting scammed.

At work, remember to report phishing attacks immediately and always follow policy.

THE DANGEROUS SIDE OF SOCIAL MEDIA

Social media: Where people connect with others from around the world, where influencers tout the latest internet trends, and where social engineers make their money. Let's review the dangerous side of social media and ways to stay safe.

Data Mining

People tend to overshare without considering the risks, which provides a great resource for scammers. For example, a cybercriminal may search social media to discover someone's interests, location, and names of friends and family. They then use this information to create scams that appear legitimate.

Stay safe: Limit what you share and set your profiles to private.

Fake Profiles

Scammers often set up fraudulent accounts that impersonate people you know. They will then send you a request to be added to your network with the intention of gaining access to everything you post, along with your entire network of connections, including friends, family, and co-workers.

Stay safe: Thoroughly vet all requests to connect and report suspicious profiles immediately.

Disinformation

Disinformation refers to any falsified information created and spread to intentionally deceive people. It's a powerful weapon that shapes public opinion for malicious purposes. Similarly, misinformation is inaccurate information that individuals share because they mistakenly believe it to be true.

Stay safe: Think critically before sharing anything that is polarizing or potentially triggering.

Deepfakes

Deepfakes are media sources like audio files, videos, and pictures that have been manipulated by technology to appear to be something they are not. The more that technology (like artificial intelligence) improves, the harder it will become to identify deepfakes.

Stay safe: As a general rule, if something sounds or looks unbelievable, assume that it's fake.