SEPTEMBER 15, 2020

VPS Article

PsyberSecurity: Where Computer Security Meets Psychology

JOHN STREFF, IT SECURITY SPECIALIST

We have all heard stories of computers being hacked, but did you know that your brain can also be hacked? High-tech computer hacking can be difficult, especially when the target organization has invested many resources into cybersecurity technologies. Because of this difficulty, many cyber-attackers have discovered that it is often easier to convince someone with access to the target system or information to share this access with the attacker (either knowingly or unknowingly). Attackers essentially "hack" the individual's brain to elicit compliance with their requests. To accomplish this, attackers use a technique known as social engineering, which relies on a phenomenon known as amygdala (pronounced uh-MIG-duh-luh) hijacking. Let's look at how this works and what you can do to prevent your brain from being exploited in this way.

The amygdala is a small structure located near the bottom of the brain and is very important in the way we process emotions. When we experience strong emotions such as fear, anger, or anxiety, the amygdala automatically triggers our fight-or-flight response, which prepares us to flee or confront the source of the strong emotion immediately and without thought. For example, think of a time someone startled you so much that your body reacted involuntarily. Perhaps your arms attempted to stop the perceived threat from coming closer. Your body reacted to the perceived threat before any thought transpired. When the stressor activates the amygdala in this way, it also inhibits the activity of the prefrontal cortex, which we consciously control to perform reasoning, critical thinking, and decision making. When the strong response of the amygdala produces an impulsive overreaction to a situation, this is known as what psychologist Daniel Goleman called an "amygdala hijack" in his book, "Emotional Intelligence: Why It Can Matter More Than IQ".

Just as computer systems have technical vulnerabilities that render them weak in the face of an attacker, the amygdala hijack can be seen as a vulnerability of humans that, when properly exploited, can manipulate an individual to take an impulsive, unfortunate action. In the context of cybersecurity, that action might involve clicking a link to a malicious website, opening a malicious email attachment, or giving attackers information that they can use in later stages of their attacks. Attackers try to create a sense of fear, anxiety, urgency, panic, or even excitement to convince their targets to act impulsively and without thinking that maybe the situation is dangerous and intended to ensnare unsuspecting users. Attackers try to take advantage of their social skills combined with our innate desire to help and trust others, especially in rural areas. These non-technical methods for carrying out cyberattacks have come to be known as "social engineering."

VANTAGEPNT.com 605-995-1777
2211 N Minnesota Street Mitchell SD 57301

A recent example of social engineering / amygdala hijacking in action is the myriad of scams relating to the COVID-19 virus. The thought of catching this virus has terrified an overwhelming number of people, and many are interested in wearing masks to protect themselves from illness. This is a great opportunity for malicious social engineers. People who are terrified of catching the virus would not hesitate to click on a link that claims to take them to a website from which they can purchase high-quality masks at an affordable price. An attacker could easily set up a fake e-commerce website that infects victims' computers with malware once they visit the site. In this scenario, the attacker creates a powerful sense of excitement that triggers an automatic, almost desperate response because of the long-term fear that has plagued the victim. The amygdala takes over and inhibits the activity of the prefrontal cortex, so the unsuspecting user does not stop to think that the link may not be legitimate.

Another common social engineering scam is offering the victim the chance to enter to win a valuable item, such as a phone. An attacker could send an email to hundreds of a company's employees offering them the chance to click on a link and enter their work computer's username and password to "verify their identity" for the registration process. Of course, attackers then collect the credentials to use in further stages of their attacks. Alternatively, some attackers send emails pretending to be technical support. These emails tell recipients that they just clicked on a link in a phishing email and that they need to download and run a program to clean up any malware on their computers and make them secure again. In reality, this program gives the attacker covert, remote access to the victims' computers. When sending these kinds of emails, attackers create excitement by offering the chance to enter a drawing, and they create fear and panic when they tell the victim about the possibility of a malware infection. Both pretexts elicit a strong emotional response and impulsive behavior. The attacker has successfully exploited the amygdala hijack vulnerability to manipulate the victims' behavior and obtain usernames, passwords, and remote access to computers.

The preceding examples demonstrate that amygdala hijacking is a simple yet effective technique for manipulating an individual to assist in carrying out a cyber-attack based on human weakness. While it may be difficult to resist these kinds of attacks, there is a way to defend yourself. If an email or phone call causes you to feel anxiety, fear, or great excitement and is asking you to do something, take a minute to relax and slow the situation down. Take some deep breaths and rationally think through the situation. Ask yourself whether the request is normal or makes sense. Ensure that the request comes from someone you trust, and do not assume the person is who he/she claims to be. Intentionally relaxing and consciously thinking will help your prefrontal cortex to regain control and help prevent bad decisions. Awareness of attackers' techniques as well as your own reactions to stress will help prevent you from becoming a victim of the amygdala hijack.

Additional Information

For more information or if you would like VPS guidance, please contact the Vantage Point Solutions banking team:

Kelly Pfeifer at (605) 995-1796, Kelly.Pfeifer@vantagepnt.com

John Streff

IT SECURITY SPECIALIST

As both a meticulous security analyst and a dedicated educator, John Streff brings tremendous strength to the Vantage Point IT Security Team. In his role as IT Security Specialist, he helps banks and credit unions secure their data networks through penetration testing, vulnerability management, policy, and other measures. Beyond technical mastery, John is especially strong at helping communicate the risks of cybersecurity breaches; and combined with his gift for training, this helps companies secure the human side of the organization – protecting entire teams and businesses from individual errors. He specializes in social engineering, security awareness training and publication, and malware analysis.

"I AM PASSIONATE ABOUT SECURITY EDUCATION AND TRAINING BECAUSE THEY PROVIDE A CRITICAL LAYER OF PROTECTION FOR A CLIENT'S CYBERSECURITY BY ENSURING SECURE USER PRACTICES."

EDUCATION

Bachelor of Science in Cyber Operations from Dakota State University, a Master of Science in Cyber Defense, and an Ethical Hacking Graduate Certificate

Kelly Pfeifer

CUSTOMER RELATIONS MANAGER

Kelly Pfeifer assumes a primary role as the problem solver for all client needs. He is committed to helping financial institutions deal with regulatory, network and security issues. Not only does Kelly provide a professional and helpful line of communication for the client, he also participates in social engineering testing. He is a master of disguise and an accomplished dumpster diver. His role as customer service manager is a central part of the financial services division at Vantage Point Solutions. Kelly double majored in Elementary Education and Business Finance at Dakota Wesleyan University. He began his career at Wells Fargo where he was twice named their top performer. He enjoys helping with Special Olympics and Junior Achievement. Kelly is also a Division I men's college basketball referee.

"I'M PASSIONATE ABOUT DEVELOPING RELATIONSHIPS BECAUSE THAT'S HOW I GET TO KNOW THE CLIENTS' PRIORITIES."

EDUCATION

Elementary Education and Business Finance at Dakota Wesleyan University