Why We Get Scammed

If you use a cellphone or have an email account, you've almost certainly been exposed to an attempt at mass marketing fraud. Common examples include being interrupted by an annoying robocall just as you start eating lunch, or waking up to a suspicious message in your email inbox that somehow slipped through the spam filter. Sometimes, the attempted fraud is kind of funny—the wording is so strange or the premise is so ridiculous ("An exiled prince needs my help transferring a million dollars? Really?") that we're left wondering how anyone could possibly fall for such an obvious money grab.

Unfortunately, mass marketing scams persist because they work—at least enough to justify the attempts made. In a 2015 Data Breach Investigation report conducted by Verizon, it was found that it takes an average of 82 seconds from the time a phishing campaign is launched for the first victim to fall for the trap.

How is it that scammers are able to trick the average person into making costly and humiliating mistakes? How is it that even the smartest people can fall for the simplest scams?

As it turns out, behind the robocalls and the cheesy emails about deposed Nigerian princes, there is some psychology at play. Scammers are very good at crafting situations that create "amygdala hijack", which is a term used to describe what happens when the brain perceives an emergency situation. Fear, urgency or threatening behaviour can trigger a reaction in your brain that sidesteps the usual neural pathways. Amygdala hijack is what compels you to act before any rational thought can kick in—and this is what many scams are designed to get you to do. In a state of amygdala hijack, you might comply with a scammer's request before your brain gets a chance to notice any red flags. This helps to explain why smart people fall for (seemingly) obvious scams.

In order to create the degree of urgency that triggers amygdala hijack, scammers rely on the following tactics: scarcity, authority and credibility.

Scammer Tactic #1: Scarcity
This is perhaps the most obvious interpretation of creating a sense of urgency: the scarcity of time. Targets are presented with a situation that requires immediate action (for example, your account will be deleted unless you enter your password now). In online sales scams, scarcity of product is often emphasized (the sales page will draw attention to the fact that there's only one product remaining at the too-good-to-be-true discounted sale price). Scarcity can also be applied to success, which plays to people's desire to benefit themselves financially. In pyramid schemes or investment fraud, a scam may be presented as a limited opportunity.

Scammer Tactic #2: Authority
Scammers will often pose as authority figures in an attempt to make demands on their targets without being questioned. Common impersonations include estate lawyers (in email scams offering a large inheritance), government representatives (in tax scams) and law enforcement

(in identity theft), but this tactic also extends to impersonating businesses (Amazon, FedEx, etc.). In email form, scammers pose as authority figures to get you to click on links or provide passwords and information without paying any close attention to the actual message or its sender. Some scammers abuse their fraudulent powers of authority further by using threatening or aggressive behavior to bully their targets into compliance.

Scammer Tactic #3: Credibility
We often look to family, friends and even other consumers when it comes to decision-making, and scammers use this to their advantage by impersonating others in order to make a scam seem more credible to its target. A common example is fake product reviews on online shopping sites. In order to move more product, the fraudulent seller will fabricate identities and post glowing reviews to influence a purchase and to bury any accurate (and negative) reviews. In other scams, existing connections are used to make a scam seem legitimate. In one especially manipulative example, scammers will use social media posts to figure out when you're out of town or on a vacation. Then, posing as you, they contact friends, relatives or co-workers and request financial help with an emergency. Because you are in fact on vacation, the request gets a little boost of legitimacy that makes it easier for targets to overlook the scam.

Even though scams come in all shapes and sizes and via different communication methods, there are some underlying similarities. Keeping an eye out for tactics like scarcity, authority and credibility will help you flag potential fraud. Even when presented with a stressful situation, create an opportunity for yourself to pause and think before acting. Although that the circumstance may seem time-sensitive, think about whether the context of the situation makes sense. Verify the legitimacy of the communication (do not use the contact information that the potential scammer has provided themselves—call them back through a main number listed on an official website). If someone is claiming to be your friend but the circumstance is suspicious, verify their identity through another form of communication, like a phone call or text message. Don't worry about being polite—verifying the identity of the person or company you are talking to is a reasonable thing to do. It also helps to take preventive measures by being careful with your personal information and using privacy settings on social media accounts.

Whether it's online, over the phone or in person, scammers are always coming up with new ways of influencing their targets to act in ways they might not otherwise. By staying calm in high-stress situations and by giving ourselves a little extra time to think, we're better able to spot recurring scammers' favorite tactics, to avoid a state of amygdala hijack and to save ourselves from making costly mistakes.