Propaganda vs. Truth

How to tell the difference

With the exponential increase in working from home, so too has gone the way of social engineering. Phishing attacks are at their highest level since 2016. Over 60,000 phishing sites have been reported in the last month alone. The bulk of previous phishing exploits centered on capturing credentials by using a fake login screen to fool users into providing their credentials, but now over 65% of phishing attacks are what is called spear-phishing. Spear phishing effectively uses a lot of information about you or your company to lull you into an inappropriate sense of comfort before attempting to get your personal information. Some phishing exploits are part of a continuum, where repeated contacts build trust and gather data about you or your company. The ultimate goal is usually to get you to eventually click on something that inevitably installs a payload or make a transaction outside of normal procedure. This is where social engineering comes in and why I want to talk about the technology of propaganda.

Social engineering is but one aspect of propaganda, as a whole propaganda enlists many tactics, but is basically a way of messaging to sway or influence opinion. In the case of cybersecurity the objective is to sway your trust, but in other spheres it can take on other objectives. In cybersecurity we know that the end user, whether they know it or not, is the biggest risk, and thus the biggest target. All the technology in the world cannot prevent a user from clicking on something they think is legitimate. Certainly, there are tools to minimize this, but even those in many cases can be overridden by the user. The National Institute of Standards and Technology Special Publications on Cybersecurity emphasizes the important of training and awareness and insider threats programs as the most effective defense against most threats. Interestingly our analysis of the effectiveness has shown that the most effective programs are ones that include practical means of discerning social engineering tactics and propaganda as a whole over other programs focused on best practices. The data shows that an educated user with sharp critical thinking skills is 91% less likely to be exploited. By contrast, users who were not given the same training clicked on a fake link 8 out of 10 times.

So how do you train a person to be able to identify propaganda over truth, and apply critical thinking to any given situation? Well, the first step to solve any problem is admitting there is a problem. We start by showing how prevalent propaganda is and how the average computer user is constantly being socially engineered, for good and bad. Propaganda is not always exploited for nefarious purposes, we see propaganda in all sorts of messaging, like branding. Advertisers also use propaganda by promoting broadcasts disguised as news – and who among us has not watched one of those at 2 AM for an hour, or clicked on what appears to be a news article only to find it is a sales pitch. But as they say, once bitten twice shy, right? Well, it depends. The term “fake news” has become a popular expression, but was in fact coined by cybersecurity experts to describe this tactic employed by advertisers. Data shows that only 70% of users who regularly clicked on misleading links were not less averse if the messaging was adequately engineered, but falls to 20% if the user received a response from the help desk that they clicked on an inappropriate link. The conclusion here is that even if we know it is likely propaganda, it is the context in which we are interacting that determines the outcome. This is no surprise of course because other research done by NIST and universities that study behavioral science also indicates that risk adversity is highly contextual. We are more prone to take risks when we are in familiar circumstances, or to take advice from a trusted friend.

The second exercise is knowing how propaganda as a technology is constructed and applied. Like a magic act that once dazzled your conception of reality, once you know how it’s done, it less magic and more trick. Propaganda is similar, once you know how it is made, it becomes easier to identify. That’s because it has a different set of attributes over trust but is applied differently in the same context. For example, you receive an email saying that a hacker has “…gained access to your systems and has your password, if you do not send money, I will erase all your files”. Is this truth or propaganda? Its hard to say right off the bat but we can make some assumptions it is likely BS. The first rule of propaganda is to have some truth so as to gain your trust in the assertion. This is the social engineering part, because we make risk decisions in context, and if there is some truth to what they are saying then maybe the rest of it is true, but we are not always conscious of that decision. In this case we are likely to dismiss this assertion, and tests prove this. But now let’s add some truth, suppose you got this message: “I have gained access to your computer and know all your passwords, to prove this here is your amazon password: xyzabc123. Now that you know I have your passwords…”. Wow, that can be scary…if that truly is your password how likely are you to believe what the hacker is asserting, and thus how likely are you to submit to the request? The answer, 3 out of 5 users will believe the hacker has all the passwords just because they knew one, even if that one password is old and wasn’t even for Amazon, and 1 out of 5 will submit to the request. As a cybersecurity expert 9 times out of 10 we know this is a lie, because (1) most hackers will encrypt your data before they ask for money and (2) pretty much every password you have used has been garnered over the years and is for sale on the deep web. But to the average user this can be very unnerving.

Let’s unpack the above example and see how propaganda works. First, we know that most propaganda will have just enough truth so that it is not dismissed out of hand, but we also know that the assertion overall is not true. Propaganda it turns out has some very distinctive attributes that differ from truth. Propaganda uses emotional trigger phrases and relies on an emotional response to cloud your judgement. Propaganda makes broad subjective statements like “…and I have all your passwords…” and “…now that you know I know…”. Propaganda tells you very directly what conclusion to come to. On the other hand truth is objective, and assertions can be independently verified.