Why Successful Phishing Attacks are NOT Random Events

WHITE PAPER

cyberconIQ

Why Successful Phishing Attacks are NOT Random Events

By Dr. James Norrie, Founder & CEO

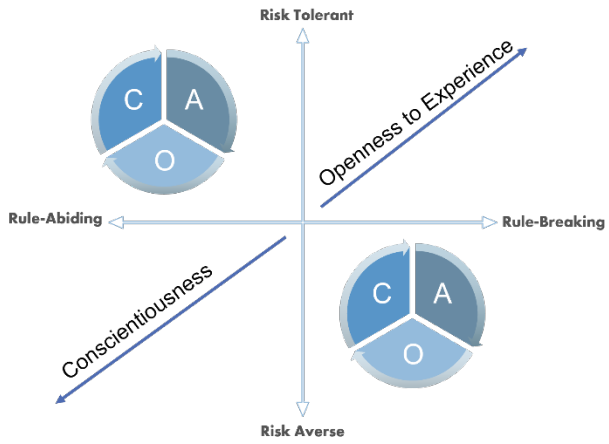
There is much emergent research conducted not only by us as embedded in CYBERology™; but also, from independent academics globally who link aspects of the "Big Five" personality traits and their potential impact on how we all behave online. There is a significant and growing body of knowledge underpinning this important theory and linking it to improved security outcomes. In fact, our InformedIQ database that underpins our research-driven approach now tracks more than 40 or more relevant clinical or applied studies over more than 10 years confirming that online employee behavior is NOT random but clearly linked in a variety of interesting ways to one or more of the five personality traits in myriad ways.

So now what? Well, we need to reimagine how we think about human-factors cybersecurity threats by adapting everything that we do as cybersecurity professionals to align to an individual's personality. Not necessarily always an easy task. However, in so doing, we can vastly improve results over any generic, one-size fits all solution and achieve important improvements that make any organizations cybersecurity resilience more durable, and that dramatically improve our external-facing cybersecurity risk posture.

On one important point, all research to date converges: there is no doubt about the connection in general between personality traits and behavior of any kind, including choices about online behavior that relate to conformance with cybersecurity policies and best practices. And particularly, many researchers have found that the Big Five traits combine to explain more or less about cybersecurity behaviors in different combinations and for different reasons at various times. This means that simply *knowing* something about any *individual's personality inclinations or trait tendencies* will inconsistently translate into practical and repeatable solutions that positively impact on cybersecurity outcomes. For a cybersecurity professional, this creates a dilemma of some complexity: how do I actually apply this theoretical knowledge in practice in a way that is scalable and reliable?

In our view, what is missing is a model that correlates specific personality traits and their strengthen of representation in any individual to their **predictable** online behavior. That

is to say, we need to link trait-based personality theory to an individual's specific vulnerabilities and train to the context of their personality and style rather than to treat content. To achieve this, we needed to perform a different kind of research that was less theoretical and more applied and concrete in nature. So we did.



Our journey to commercializing and patenting our products began with a simple research question: could we predict which particular vulnerabilities were more or less triggering based on particular personality traits? And to our delight, we found out that we could. In fact, we found very high correlations between specific personality traits and online attacks.

We determined this by analyzing **vulnerability and threat exposures compared to actual failure data from real users.** To accomplish this, we used the standard threat taxonomy provided by the Internet Crime Reporting Centre (IC3) to classify threats and their prevalence. Over time, we were able to link specific patterns of online behavior that resulted in compromise back to aspects of personality as defined using the Big Five model. Particularly we defined the simple idea that risk and reward, and the intention to follow rules or not, are endemic to one's personality and not random occurrences in any particular moment and where highly correlative to specific threats that consistently triggered personal vulnerability to specific vectors of attack. This means that *every quadrant is vulnerable in different ways, and relatively more or less risky as a result.* However, each quadrant is also associated with different contributions and value they bring to the workplace and so they are all absolutely necessary as well. Essentially, by understanding the make-up of these styles across your organization, you can essentially measure your particular Cyber "Risk DNA" actually.

That is because there is reliable predictability to each quadrant's online behavior. Our research design, since repeated many times, enabled a practical and reliable model of four quadrants into which almost everyone falls. And each quadrant then has varying levels of vulnerability to specific kinds of cybersecurity threats as a result of the singularity or mixture of Big Five personality traits associated with each quadrant. Our proprietary model offers cybersecurity practitioners a highly reliable, simple and scalable method to apply the Big Five personality traits to predicting individual online behavior.

In our particular model, and in keeping with what many other researchers have also found, three of the five traits had particular relevance to online behavior: **conscientiousness, openness to experience and agreeableness.** Our model has not

detected any significant correlations to extroversion or neuroticism that were reliable enough to include. That said, we are constantly evolving our model based on actual client experience, new research findings and confirmation of findings in practice as new threats and vulnerabilities emerge. As a research-driven company, we always endeavor to keep our models up-to-date as actual client experience dictates the release of new findings, tools or methodologies related to our instrument or as new theoretical research emerges that indicates new opportunities to improve.

So, having established that our myQ questionnaire was a valuable method to categorize and predict their online behavior, there were some other things to consider in order to make the model approachable and useful in an enterprise setting. First we gave each quadrant a "playful" name and created aligned descriptions that were tested with hundreds of individuals over time to ensure they self-reported a high degree of acceptance about their own quadrant's description. This is important for validity. And we created a secure and simple online application using only 40 questions and about 10 minutes of anyone's time for them to be able to self-locate in the quadrants accordingly.

In the bottom-left quadrant of our model are those whose personality is dominated by being conscientious. As a result, they are risk-averse, cautious and careful in all that they do and they pride themselves on following the rules and adhering to policy. This makes them both vigilant and compliant and sensitive to anything that is out of the ordinary. This renders them practically immune to obvious vectors of online attack that they simply will not fall prey to. In our experience, this quadrant is relatively least risky and most responsive to rules-driven cybersecurity policies that simply inform them of what they should and should not do. Yet, while this is a strength, like any personality trait, a strength taken to an extreme becomes a disadvantage and so it is with this quadrant's almost obsessive conscientiousness. They are absolutely highly vulnerable to hybrid attacks, particularly those involving impersonation of authority, because if told to break the rules by someone in authority, they often will. If you taint that threat with content suggesting that they have not been attentive to a request or have not conformed to expectations, this unsettles their nature and makes them quite vulnerable in the moment. So, when presented with certain types of attacks, this group will almost always fall for them. And for other types, almost never.

In the top left-hand corner, we found an intriguing quadrant that has a unique blend of the three traits. While conscientiousness is still an important part of their personality, these individuals demonstrate more willingness to take calculated risks when faced with evidence of value in so-doing. This arises as a result of higher degrees of agreeableness making them more sensitive to requests to break the rules arising from others. This quadrant is also relatively less risky generally and remain fairly vigilant against those threats that on the surface just seem "too good to be true".

However, in practice we have discovered that when you add in urgency or emergency, you can provoke a decrease in that vigilance and increase their vulnerability in the moment to particular threat vectors, especially those involving threats to persons, property, family, key client relationships or the loss of prestige or which threaten exclusion or intrusion unless they act. This is particular to the make-up of their personality of course, and by linking these inherent impulse instincts to new training, we can reduce their sensitivity by teaching them to spot this innate response and suppress it with a planned inclination instead. This means training and supervising them differently than by simply reciting the rules you expect them to follow, and instead focusing on exceptions to rules.

Now we move across to the top-right quadrant, a relatively riskier quadrant statistically speaking! As we cross over the rule-breaking inclination, we find individuals who are both risk tolerant, if not even risk seeking, and also quite willing to break the rules. These folks easily challenge the status-quo, are creative and daring. This is because their personalities are completely dominated by an openness to experience. They have learned over time to trust their instincts and they feel that this has benefited them and so there is an unwillingness to consistently follow the rules by nature. It is this quadrant for whom existing cybersecurity training paradigms most fail to inspire any change in behavior or recognition of the value of even following rules or policies until they have personally concluded would be valuable in practice. This skepticism of rules is endemic to personality and not intended as an evasion of policies or rules, although it may seem like this is the root cause. Again, in years of experience now with this quadrant, we have also discovered an interesting characteristic: because they tend not to be detail-oriented (as a result of not being contentious by nature), they tend to surround themselves with people they trust to "sweat the details" on their behalf. This creates a high degree of trust that is, understandably, easily exploited by certain online threats that involve being attacked through a trusted source (such as man-in-the-middle; affiliative attacks arising from organizations or groups to which they belong; or socially-engineered attacks that mimic trusted members of their own teams for instance). In our focus groups, we have learned much about how to influence the behavior of this quadrant by invoking a sense of purpose around their behavior as a role model for others for example that appeals to the make-up of their personality and engenders more awareness of particular reasons why they should deviate from relying entirely on their own judgement when assessing online threats. In various experiments, we have also concluded that simple rule-based training will not ever accomplish anything other than temporary changes in behavior or limited periods of time normally right after the training. This is the result of short-term sensitization and not a fundamental long-term change in behavior that will only be accomplished by understanding their style and modifying interventions accordingly to peak their interest in new experiences as a way to learn.

We now come to our last quadrant in the bottom right corner. Again, we find a quadrant that is not dominated by a single trait but which is a mix of the traits that produces someone who is absolutely willing to break the rules – in fact, they love the autonomy to decide when they will and will not follow the rules – but for whom the appearance of being rule-abiding is socially important because they are also not inherently risk tolerant and they fear exposure of having broken the rules in consequence. This is the result of higher degrees of both agreeableness and openness to experience in their personalities rather than contentiousness'. Many of us when working with individuals in this quadrant have concluded they are complex and intriguing by nature, quite good a problem solving and describing complex problems in simple terms and are often reported as being lots of fun to be around although they are not uniformly extroverted either in our research to date. However, from a cybersecurity perspective, this is relatively the riskiest quadrant because their willingness to break the rules while having a desire to remain covert often makes them more vulnerable to a variety of common online attack vectors which involve shaming, extortion, or manipulation of their fear of discovery that are rampant currently. We have also found that, once again, simply rule-based training will almost invariably fail to inspire sufficient behavior change to avert these threats unless you are willing to be direct and clear with them about these risks. Our research and experience suggests lots of simulation and scenario-based training delivered in a way that permit exploration of alternatives safely as an effective intervention that more consistently increases their self-awareness of their personality traits for specific cybersecurity threats and vulnerabilities. This ability to detect that connection makes them more willing to stop and reach out at critical points before they are already down the slippery slope of an attack when its often too late.

So, our model is emergent and continues to evolve with experience and additional research. However, it can significantly reduce your organization's probability of a human-factors attack. To prove our point, let's just consider one isolated example of ransomware, a potent threat that is absolutely devastating if your organization is attacked. Of course, to be effective, the ransomware payload must first reach an employee. With modern technical tools, appropriate threat intel and good cyber hygiene practices, many of the most common payloads will be identified and deflected at the point of entry today. For most of our clients with fairly mature cybersecurity programs, they can repel 80-90% of most typical threats like this. Depending on the size of the organization, this still leaves a significant number of either novel or undetected new threats reaching your employees, likely using attack vectors like business email compromise, or smishing, vishing or whaling attacks derived from social engineering for example.

It is at this point that you are counting on your human firewall to avert disaster. You must consistently and constantly enhance your employees' ability to spot these attacks, and

both avert them and report them. Without that last line of defense, your organization is vulnerable, and the likelihood of an attack remains quite high given the intense threat landscape currently being experienced with sophisticated foreign-based cybercrime gangs turning ransomware into a scalable crime-as-a service opportunity.

If you only undertake generic training, or training which is role or access-based, you are missing a potentially valuable opportunity to reduce risk. Why? Because it is NOT the fact that someone has a particular access level or is in a position that is being targeted because of its likely access to information. Rather, it is understanding that the personality of people in those roles is different and that, at any particular moment, each of them is vulnerable to a different vector of attack *by nature* and that to make them more aware requires that we understand *what they are vulnerable to and why* if we want our cybersecurity training effectiveness to improve. In our practice, we refer to this as "style-aligned" training which is based on the quadrants previously described and which in side-by-side controlled, randomized experiments – essentially the gold standard of scientific research – we have demonstrated 4x-6x more effectiveness at employees willingly changing their on-the-job behavior in such a way that it mitigates more threats more quickly when they are exposed to them. In effect, we train them to spot their own vulnerabilities based on personality and to self-correct behavior to avoid risk.

Is it perfect? Absolutely not because psychology itself cannot never be perfect either. Much of its value has simply to do with impacting how individuals think about themselves and the world in which they live. However, our model is very stable and does reliably explain a significant amount of variation in behaviors that tied to risk vulnerabilities better than any existing alternatives. That is because we embed the latest and most up-to-date research on connections between the Big Five traits and online behavior. And because we have a model that can identify the presence and strength of these traits in your employees, you can start to use this important information in a variety of new ways well beyond just training. Our consulting teams have helped clients use them to improve DevSecOps compliance within IT professional teams for example. Or to use them in their SOCs to better perform initial incident triage to accelerate human intervention on threats which are not symmetrical to style, and which may represent immediate danger. Or to assess secondary controls that may be helpful when someone remains vulnerable on the basis of personality and is unlikely to be remediated exclusively by training.

We do not yet even know ourselves how far this model can take us. But we do know this: it can take us much further than most cybersecurity programs can go today without embedding trait-based personality theory into them. And that gives us some hope that this approach can really make a difference and keep our clients safe and more secure online.

Learn more at www.cyberconIQ.com