Research Report

Does personality enhance susceptibility to cyber attacks?

Dr. Inka Karppinen
Behavioural Scientist, CybSafe

Isabella Houghton
Research Analyst, CybSafe

Ananya Saha
Research Analyst, CybSafe

Dr. John Blythe, CPsychol
Head of Behavioural Science, CybSafe

www.cybsafe.com
CONTENTS

Introduction 3

Personality research in cyber security 4

Deep dive of the Big Five personality traits 5
Openness to experience 6
Conscientiousness 6
Extraversion 7
Agreeableness 7
Neuroticism (Emotional stability) 8

Potential personality links with cyber security 9

Is personality profiling ethical? 12

The future of personality and cyber security 14

Conclusion 16
Introduction

In the current economic climate, it’s important to continually manage cyber risks. Traditionally, people have been seen as the weakest link in cyber security. Such thinking is now outdated. Many now agree that people are our best defence. Equipping people with the skills they need to protect themselves and their organisations is vital. Through a positive psychology lens, we can move away from seeing people as a “security problem” that needs fixing. We cannot “fix” human error or change human irrationality. So how could we address people’s poor security behaviours? Many are moving towards empowering people, and harnessing their strengths and differences. Their aim is to build a positive and personalised experience for all.

One underlooked area is the role of personality traits. These are the aspects that determine how people think, feel and behave. What makes us different from one another? What role does personality play in cyber security? Do personality traits make us more susceptible to cyber crime? And most importantly, can we use personality to improve cyber hygiene?

CybSafe in collaboration with the NCC Group have started a series of human factors research papers on the topic of personality traits and digital footprints. Through our initial research, we’re beginning to understand these unexplored areas. At the same time, we’re calling for other researchers to examine personalised approaches to human cyber risk.

In this paper, we’ll discuss the role of personality in cyber security, drawing on a wealth of academic research. We’ll use the Big Five personality model to explore personality traits that practitioners could harness in cyber security training. Finally, we’ll highlight not only the benefits but also possible challenges in their application.
Personality research in cyber security

Personality research in cyber security helps explain why different people make different security decisions. Using this information, we can tailor programmes to specific audiences to maximise effectiveness. This is much like making a made-to-measure suit. Tailor-made suits fit perfectly. Generic suits do not – no matter how fine the underlying fabric might be.

Your personality is a combination of several traits that exist in a continuum. These traits determine your thoughts and decisions in everyday situations. The earliest personality research dates back to 400BC1 and sets foundations for today’s Big Five Model of personality. It’s the most common personality model in the cyber security industry2. It has also attracted a wealth of scientific interest from a wide variety of cultures3.

1 Hippocrates Four Temperaments https://psychologia.co/four-temperaments/
Does Personality Enhance Susceptibility to Cyber Attacks?

Deep dive of the Big Five personality traits

The Big Five Model consists of five traits. These are Openness, Conscientiousness, Extraversion, Agreeableness and Neuroticism (OCEAN, see table 1).

These traits are all continuums, upon which a person may “score” high or low. Make no mistake, the traits are complex. This means no proficiency in any trait can be viewed as good or bad. The traits have their own strengths and weaknesses that may be linked to moods or events. For example, stressful life events can increase our neuroticism.

<table>
<thead>
<tr>
<th>Big Five Trait</th>
<th>Associated personality attributes (where high scores indicate):</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Openness (to experience)]</td>
<td>Intellectually curious, imaginative, novelty-seeking, open-minded, adventurous, independent, creative, emotionally self-aware, artistic</td>
</tr>
<tr>
<td>![Conscientiousness]</td>
<td>Trustworthy, organised, consistent, task-focused, dependable, methodological, able to control impulses, orderly, tenacious, self-effacing, dutiful, achievement-striving, self-disciplined, cautious</td>
</tr>
<tr>
<td>![Extraversion]</td>
<td>Enjoys company, optimistic, energetic, assertive, warm, excitement-seeking, ambitious, gregarious, friendly, high activity-level, cheerful</td>
</tr>
<tr>
<td>![Agreeableness]</td>
<td>Trusting, compassionate, compliant, likeable, cooperative, emotionally responsive, modest, considerate, moral, altruistic, sympathetic</td>
</tr>
<tr>
<td>![Neuroticism (Emotional stability)]</td>
<td>Impulsive, prone to stress and anxiety, self-conscious, sceptical, immoderate</td>
</tr>
</tbody>
</table>

Table 1: Big Five traits and their associated personality attributes.

Studies⁴ have found strong links between personality traits and security behaviours. For example, agreeableness and conscientiousness have been linked to better cyber security practices. Below we cover how each personality trait relates to cyber security.

---

People who score higher on openness to experience have been found to be relatively vulnerable to phishing scams. They often tend to follow cyber criminals’ demands. But the research also shows that a variety of interactions might have prepared open people to handle unexpected stimuli. This is largely supported by their adventurous sub-trait. Both passion for change and preference for routine enhance the ability to recognise when something is out of the ordinary. This is useful when detecting unusual emails.

Another sub-trait, liberalism, could also influence people’s security behaviour. The liberal can challenge the authority as well as rules and regulations. In cases, this can hinder adoption of security policies.

The openness trait might be protective when faced with online scams. But it could be damaging to a workplace culture if not handled carefully.

Overall, relatively conscientious people face decreased cyber risk because they comply with rules and regulations. Research has shown that conscientious people are more likely to update software regularly and generate strong passwords. Conscientious people can be achievement-striving. This might result in believing a phishing email in the spur of the moment, especially if already under pressure.

---


This trait is often shown in a positive light. But people with high extraversion scores can also be vulnerable to cyber attacks. They tend to have outgoing personalities and respond to rewards and social attention. These are techniques used by criminals in social engineering attacks.

In busy workplaces, extraverts are more likely to violate security policies as they try to get their tasks done. That said, research shows that extraverts tend to be more diligent in securing their devices. Also, with their inner need to communicate, they can be assertive and speak out about security breaches. This could help organisations identify breaches and foster a security-oriented culture.

Highly agreeable people are more likely to fall for cyber attacks. They tend to have trust in others, which cyber criminals may exploit. Phishing emails that give agreeable people the chance to help others are often their pitfall.

Agreeable people have been shown to be very security-conscious. Research suggests that agreeable people are better than most when it comes to detecting deception. They display high levels of workplace commitment and high security awareness. Their cooperation encourages reporting behaviour and they tend to use security software.

---


Often portrayed in a negative light, neuroticism can be beneficial when it comes to cyber security. Individuals with higher neuroticism scores have been shown to have a decreased phishing susceptibility\(^{17}\).

Research shows that neurotic people excel in distinguishing genuine emails from phishing emails. A relative lack of online exposure may protect conscientious people further from online scams and social engineering attacks\(^{18}\). Yet, high scorers should be careful not to make hasty decisions in anxious situations. When faced with a carefully crafted, urgent-sounding scam attempt, it can be easy to make unsafe choices in a moment of panic.


DOES PERSONALITY ENHANCE SUSCEPTIBILITY TO CYBER ATTACKS?

Cyber security opportunities and vulnerabilities of personality

Every personality trait has potential opportunities and vulnerabilities that can be associated with them.

In this section, we outline potential security personas for each personality trait. These are based on findings from academic research to date. The research, however, has been mixed and much work is needed to further explore these in more depth.

<table>
<thead>
<tr>
<th>Personality Trait</th>
<th>Opportunities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Openness to experience</td>
<td>Fast and curious learner when it comes to cyber security topics</td>
</tr>
<tr>
<td></td>
<td>Tends to detect suspicious activity</td>
</tr>
<tr>
<td></td>
<td>Spots phishing emails quickly</td>
</tr>
<tr>
<td></td>
<td>Likely to be receptive to training offering variety of information and media types</td>
</tr>
<tr>
<td>Conscientiousness</td>
<td>Examines information</td>
</tr>
<tr>
<td></td>
<td>Concerned about privacy</td>
</tr>
<tr>
<td></td>
<td>Completes training</td>
</tr>
<tr>
<td></td>
<td>Quick to spot suspicious emails</td>
</tr>
<tr>
<td></td>
<td>Installs software updates</td>
</tr>
<tr>
<td></td>
<td>Uses password management strategies</td>
</tr>
<tr>
<td></td>
<td>Likely to be receptive to training following norms and rules</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Personality Trait</th>
<th>Vulnerabilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Openness to experience</td>
<td>Less concerned about privacy</td>
</tr>
<tr>
<td></td>
<td>Looking for the variety might find that the standard security training is not worth their time</td>
</tr>
<tr>
<td></td>
<td>Likely to comply with the criminal’s demands if they seem genuine</td>
</tr>
<tr>
<td>Conscientiousness</td>
<td>When under pressure can be susceptible to phishing</td>
</tr>
<tr>
<td></td>
<td>Susceptible to spear-phishing where genuinely-looking scams offer achievements or prizes</td>
</tr>
</tbody>
</table>
DOES PERSONALITY ENHANCE SUSCEPTIBILITY TO CYBER ATTACKS?

### Extraversion

**Who am I?**
Social chatterbox, who thrives in the company of others

“**I’m goal-focused people’s person. Others describe me as energetic, outgoing, and gregarious**”

**Opportunities**
- Complies with security training and procedures
- Installs software updates and secures devices
- Diligent in securing and updating devices regularly
- Tends to speak out any security issues
- Encourage others to complete training
- Likely to be receptive to training that highlights social aspects, game-like features and being able to share knowledge

**Vulnerabilities**
- Less concerned about privacy
- High social activity can lead to disclosure of sensitive, personal information
- Susceptible to phishing scams that offer rewards, deals or social recognition

### Agreeableness

**Who am I?**
Cooperator, who fosters relationships

“I enjoy teamwork and helping others. Others view me as considerate and compassionate”

**Opportunities**
- Follows security policy
- Takes information onboard around cyber security topics
- Installs software updates
- Spots phishing emails quickly
- Reports security breaches diligently
- Likely to be receptive to training that emphasises morals and when viewing training as common good

**Vulnerabilities**
- Vulnerable to spear-phishing especially when messages are friendly and come from authoritative sources and/or appeal to their compassionate nature
### Neuroticism

**Who am I?**
Evaluator, who is practical and grounded in reality

“I focus on the task at hand and analyse through a critical lens. Others view me as self-aware and realistic”

<table>
<thead>
<tr>
<th>Opportunities</th>
<th>Vulnerabilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Focus on minimising risks</td>
<td>• Under pressure and in situations triggering anxiety can make hasty judgements especially when faced with persuasive or urgent phishing attempts</td>
</tr>
<tr>
<td>• Concerned about privacy</td>
<td>• Colleagues’ views can influence whether security training is completed. Less likely to complete if talked about as an unnecessary task</td>
</tr>
<tr>
<td>• Lower trust on others can act as a safeguard</td>
<td></td>
</tr>
<tr>
<td>• Fewer online interactions</td>
<td></td>
</tr>
<tr>
<td>• Likely to be receptive to training showing how to lessen the worry and anxiety</td>
<td></td>
</tr>
</tbody>
</table>
Is personality profiling ethical?

Personality profiling has been used in identifying job suitability, recruitment and employee development. Using personality traits to determine career prospects has been debated widely in the social science fields. Even so, recruiters today use personality tests to ensure candidates ‘fit’ certain roles. For example, interpersonal skills are an asset in sales and managerial roles, which are part of the extraversion trait. Big Five traits are also useful in job-related areas other than task-performance. Examples include leadership skills, training performance, organisational citizenship behaviours and counterproductive behaviours.

The use of self-report surveys in hiring contexts is often criticised due to the social desirability bias. Here, surveys can become inaccurate when participants lie. One could overcome the social desirability bias by collecting information in an objective manner. For example, through a person’s online presence. Indeed, employers have used social media platforms to learn about people’s personality traits.

It’s noted that those high in extraversion and agreeableness scales tend to post photos with others and are more expressive (e.g. smile). To increase the accuracy of the digital footprints, demographics (e.g. age and gender) and a variety of digital platforms have been combined. This has opened up the possibility of misuse of such data.


Digital records (e.g. Facebook, browsing history and search queries) can include sensitive data (e.g. sexual orientation)²⁵. These can be easily accessed without a person’s consent. They can be further used in targeted advertisements. They can even be used to garner more voters in elections. Data collection must therefore be transparent. Indeed, this was a lesson learned by Cambridge Analytica.

Cambridge Analytica used ‘psychographic targeting’ harnessing Big Five personality traits to deliver tailored messages. They collected Facebook users’ data without explicit consent through a third-party application. 300,000 people downloaded the application. Unknown to them, downloaders ended up sharing their own data as well as their friends’, adding to a dataset that included 87 million people. The personality trait data was then used during the US Presidential election campaign in 2016. Here, campaigners attempted to persuade voters by tailoring messages to personalities.

The data sets have since been deleted. But the Cambridge Analytica scandal is a reminder of how vulnerable people are in digital environments. It shows how easily information can be ‘mined’ online without consent or full understanding of what a person agrees to share.

While we could use ‘psychographic’ profiling in cyber security awareness, we must be transparent. People must be aware of how their information is used, stored and how they can change data or delete it completely. Trust is really important in cyber security.

---

The future of personality and cyber security

Much of the research on personality types and susceptibility to cyber attacks is mixed. This points to the challenges of using personality traits in cyber security training in an actionable way. A possible reason for this may be insufficient interest in experimentation with a model where the traits exist in a continuum (e.g. Big Five). Also, fairly flexible sub-traits and self-reported personality surveys fuel research disagreements.

Various blogs and white papers have been written by the commercial personality test-developers. These have attracted interest in this topic, but at the same time, the advice offered tends to be vague. Instead of offering tailored advice to suit each trait, the cyber security behaviours under each trait are the same. This further renders the use of personality measures meaningless in cyber security. Here, we risk reverting back to one-size-does-fit-all mentality. Definitely, there is a lot to do here.

Personality traits are seen as the novel concept and somewhat unexplored territory in practice. The research is often conducted with student samples and not easily generalisable. It would be interesting to incorporate such elements into workplace training programmes. This could be done by adding a brief personality inventory (e.g. 44-item BFI26) to tailor the types of security threats presented to a learner. Additionally, we could tailor the training modules to suit the learner’s personality trait. Here, the learner receives content that appeals to their individual differences in personality. For example, extroverts would receive content that appeals to their social preferences.

Those people that score high on the openness to experience scale could prefer a variety of visuals instead of relying on the text.

Larger personality inventories (e.g. IPIP 120\textsuperscript{27}) assess the sub-traits of the Big Five. This offers the potential to pinpoint groups of people who could benefit from rewards-oriented security programmes.

For example those with high scores on immoderation and achievement scales. Additionally, people scoring high on intellectual curiosity\textsuperscript{28} (part of the openness to experience scale that measures one’s interest in abstract things) could be offered security modules that are more focused on problem-solving (e.g. puzzles). Conversely, those with lower scores find more relevance with programmes that focus on actual people and real-world examples.

Steering away from the one-size-fits-all training and tailoring security programmes have been the top of the agenda for some time now. The ability of a tailored programme to target specific issues and adapting to learner’s needs has positively aided the individual’s learning process. Indeed, we can use personality traits in the wider learning and development context to help people in understanding their preferred learning methods.

There exists a potential to link personality with various professions people select. This offers opportunities to further tailor cyber security programmes (e.g. phishing) to lower the risk faced by various people. We acknowledge that combining personality research and cyber security requires a large amount of work. We welcome comments, investigation of its usefulness and call for more research into this area.

\textsuperscript{27} https://www.personalityassessor.com/ipip120/

\textsuperscript{28} It is important to emphasise that this trait is not the same as intelligence or IQ but is about how one likes to experience the world.
Conclusion

The risk of falling victim to a cyber attack has increased with cyber criminals adopting novel and unexpected tactics. It’s important to act on the security vulnerabilities within IT systems, but we should also strengthen our defences through the people at the workplace. Understanding their security behaviours and everyday decisions is crucial. While cyber security training is often part of the IT and compliance department responsibilities and offered as a standard training across the workforce, the effect of one-size-fits-all training is often short-lived.

In this paper we discussed the role of personality in cyber attacks, the opportunities and vulnerabilities of specific personality traits and examined the ethical and practical implications of personality in cyber security.

We welcome more research work to explore how best to harness personality within awareness, behaviour and culture change campaigns.
About CybSafe

We are CybSafe. A British cyber security and data analytics company. We make it easy to manage human cyber risk.

Our software gets people engaged in security. It empowers them to make the best everyday-security decisions possible. We use behavioural science, data and reporting metrics to help security professionals do their jobs better. And see their impact on people-related cyber risk.

Our customers report improved security habits and fewer people-related security incidents.

About NCC Group

NCC Group exists to make the world safer and more secure. As global experts in cyber security and risk mitigation, NCC Group is trusted by over 14,000 customers worldwide to protect their most critical assets from the ever-changing threat landscape.

With the company’s knowledge, experience and global footprint, it is best placed to help organisations assess, develop and manage their cyber resilience posture.

To support its mission, NCC Group continually invests in research and innovation, and is passionate about developing the next generation of cyber scientists.

With circa 2,000 colleagues in 12 countries, NCC Group has a significant market presence in North America, Europe and the UK, and a rapidly growing footprint in Asia Pacific with offices in Australia, Japan and Singapore.