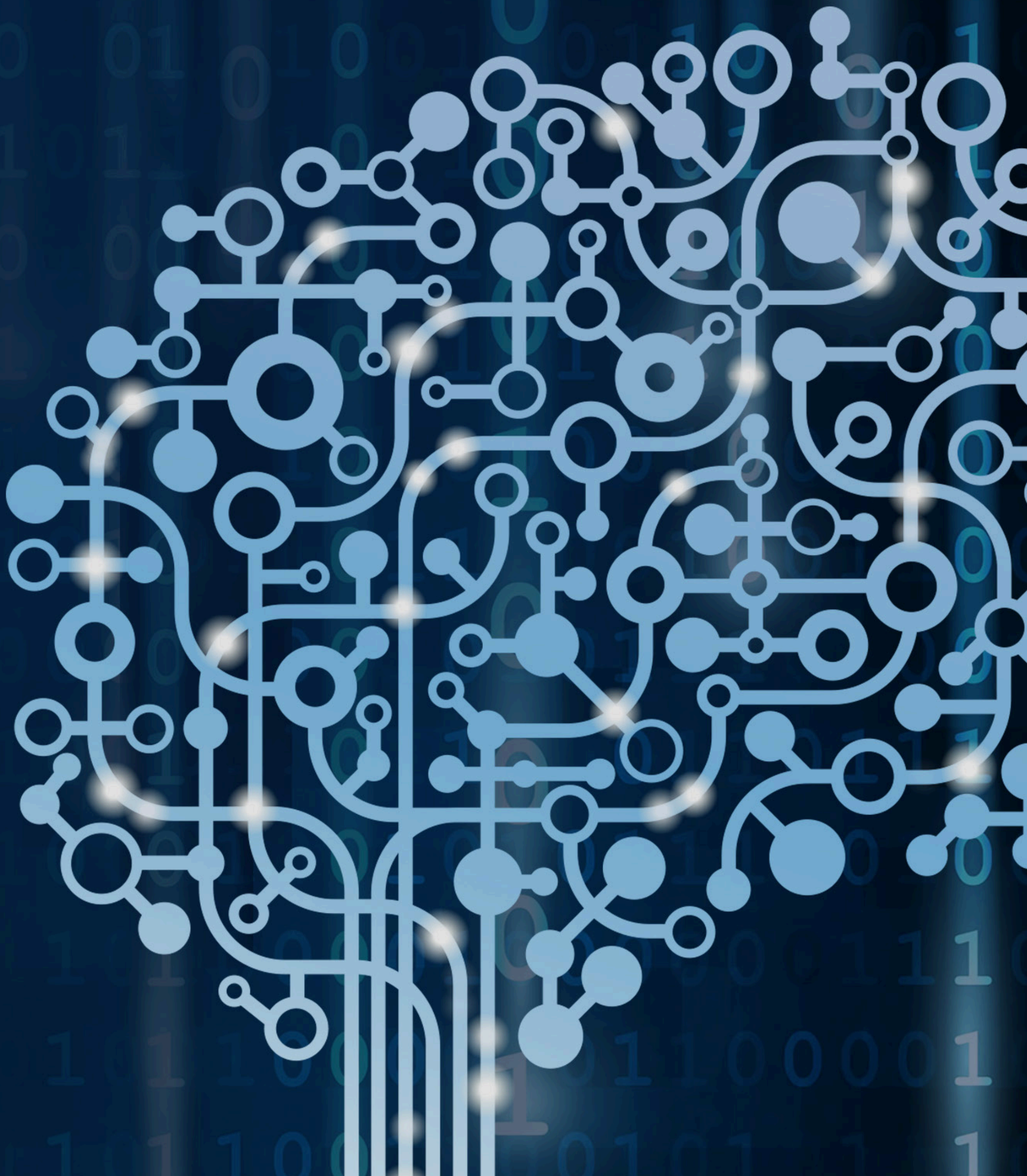
BIOCATCH™
Less Friction. Less Fraud.

BioCatch White Paper

Deconstructing the Cyber-Psychology Behind Behavioral Biometrics

September 2017



www.biocatch.com

Less Friction. Less Fraud.

Deconstructing the Cyber-Psychology Behind Behavioral Biometrics

Contents

In recent years, a body of literature has amassed on the promise of behavioral biometrics and various facets pertaining to its applications: *Identity Proofing, Continuous Authentication and Fraud Prevention*. Prevalent discussions include: frameworks for transparent authentication through user touch behavior;[1] behavioral biometrics used to detect computer intrusions;[2] behavioral biometrics for human identification;[3] identity theft and behavioral biometrics;[4] and behavioral biometrics for continuous authentication.[5]

To date, however, the literature on behavioral biometrics has mostly overlooked one of the foundations of this technological approach: the cyber-psychological determinants (affective, behavioral, cognitive) that drive human behavior while interacting with computers/devices. The following piece will examine a plethora of psychological drivers behind online user behavior that BioCatch's solution is able to identify, collect, quantify and process for authentication and fraud prevention.

We will also argue that the real power of behavioral biometrics lies in the ability to understand human-computer/device interactions, the drivers behind unique user behavior and applied methods for behavioral biometric analysis. All these amalgamated in one solution, create a powerful tool that can effectively reduce fraud and provide online/mobile users with a frictionless experience.

Introduction to Cyber-Psychology

Cyber-psychology is an emerging research program which examines individuals in the context of human–technology interactions. As a developing field, cyber-psychology relates to several psychological phenomena associated with or affected by technological applications and use. Essentially, research topics include human–computer interaction: computer graphics, operating systems, programming languages, communication theory, graphic and industrial design disciplines, linguistics, social sciences, cognitive psychology, and human performance. While some researchers emphasize the computer in computer–human interaction, a defining characteristic of cyber-psychology is that the human takes precedence over the computer.

Kent Norman in *Cyberpsychology: An Introduction to Human–Computer Interaction* discusses numerous topics in the psychology of human–computer interaction, and provides the following definition:[6]

> *"Cyber-psychology is about humans and computers and the psychology of how they interact. Computers permeate nearly every human activity in the modern world and affect human behavior from the most basic sensory-motor interactions to the most complex cognitive and social processes"*

[1] C. Bo, L. Zhang, X.Y. Li, Q. Huang and Y. Wang, "Silentsense: Silent User Identification via Touch and Movement Behavioral Biometrics," Proceedings of the 19th Annual International Conference on *Mobile Computing & Networking* (2013): pp. 187-190.

[2] A.A.E. Ahmed and I. Traore, "Detecting Computer Intrusions Using Behavioral Biometrics". In PST (2005).

[3] L. Wang, ed., *Behavioral Biometrics for Human Identification: Intelligent Applications: Intelligent Applications.* IGI Global, (2009); K.O. Bailey, J.S. Okolica and G.L. Peterson, "User Identification and Authentication Using Multi-Modal Behavioral Biometrics." *Computers & Security*, 43, (2014): pp.77-89; H. Saevanee and P. Bhatarakosol, "User Authentication Using Combination of Behavioral Biometrics Over the Touchpad Acting Like Touch Screen of Mobile Device". In *Computer and Electrical Engineering, ICCEE 2008. International Conference* (2008): pp. 82-86.

[4] R. Moskovitch, C. Feher, A. Messerman, N. Kirschnick, T. Mustafic, A. Camtepe, B. Lohlein, U. Heister, S. Moller, L. Rokach, and Y. Elovici, "Identity Theft, Computers and Behavioral Biometrics. In Intelligence and *Security Informatics, 2009. ISI'09. IEEE International Conference*, (2009): pp. 155-160.

[5] I. Deutschmann, P. Nordström and L. Nilsson, "Continuous Authentication Using Behavioral Biometrics." *IT Professional, 15*(4), (2013): pp.12-15; C. Bo, L. Zhang, T. Jung, J. Han, X.Y. Li and Y. Wang, "Continuous User Identification via Touch and Movement Behavioral Biometrics." *Performance Computing and Communications Conference (IPCCC), 2014 IEEE International*, (2014): pp. 1-8.

[6] K. L. Norman, *Cyberpsychology: An Introduction to Human-Computer Interaction* (Vol. 1). New York, NY: Cambridge University Press, (2008).

Part 1: Identity Proofing

Identity Proofing establishes the uniqueness and validity of an individual's identity to facilitate the provision of an entitlement or service, and may rely upon various factors such as application fluency, navigational fluency and data familiarity.

Application Fluency: Most fraudsters use compromised or synthetic identities to repeatedly visit a site. These actions show a fluency with the site and the process used to open a new account. One way of detecting fraud in real-time is by examining the time it takes to fill out an online application. Typically, a genuine new user will require more time to complete the application, whereas, a fraudster who repeatedly attacks a site will do it much faster since he is well-acquainted with the application.

Navigational Fluency: Fraudsters often use advanced computer skills that are rarely seen among real users. Common examples include keyboard shortcuts and function keys.

Data Familiarity: Another way of detecting fraud in real-time is by examining the level of data familiarity by the user. Genuine users are usually very quick with fields that include personal information, such as names, addresses, etc. Behavioral biometrics can detect anomalous behavioral patterns by examining whether users frequently make mistakes on details that should be intuitive.

BioCatch employs several cyber-psychological concepts in the solution for identity proofing:

Intuitive vs. Computational User Responses

Cognition is a tale of two systems of the mind, or what is now known as *Dual Process Theory.*[7] Cognitive psychologists have been intensely interested for three decades in two modes of thinking: *Intuition and Computation*, or also labeled as, *System 1* and *System 2.*[8] *System 1* is the automatic, rapid, lacking a sense of voluntary control, intuitive-heuristic mode. *System 2* is the effortful, deliberate and demanding, computational-analytic mode. In the activation of System 1, heuristics are employed to assess situations, probabilities and to predict values.[9]

System 1	System 2
Rapid	Slow
Automatic	Controlled
Intuitive-Heuristic	Computational-Analytic
Subconscious Reasoning	Conscious Reasoning
Effortless	Effortful
Implicit	Explicit
Independent of working memory	Limited by working memory capacity

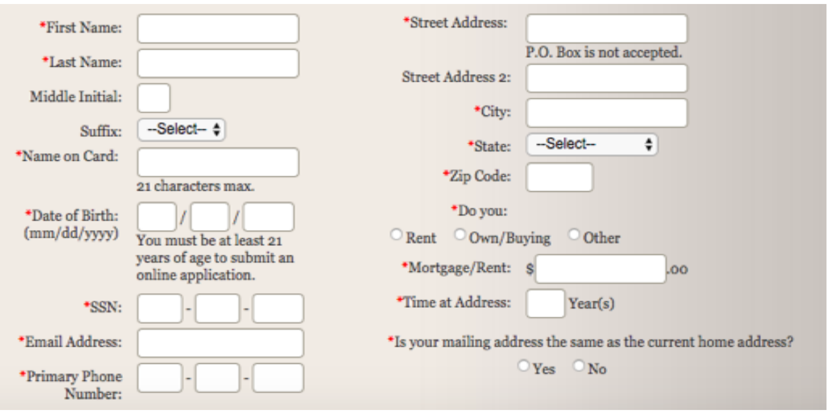
When genuine users fill out e-forms that ask for intuitive personal information like names, addresses, phone numbers, name on credit card, *System 1* is in play. Hence, they respond very quickly in these fields.

On the other hand, fraudsters will most likely be guided by *System 2*, and their responses will be different. An in-depth analysis of fraud files and user behavior shows that fraudsters frequently make mistakes on details that should be intuitive and entering information in these fields is much slower than genuine users. Behavioral biometrics can detect these anomalies through data familiarity analysis in new account fraud attempts.

[7] J. Evans and K. Frankish, eds., In *Two Minds: Dual Processes and Beyond.* Oxford: Oxford University Press (2008).

[8] D. Kahneman, *Thinking, Fast and Slow.* New York: Farrar, Straus and Giroux, (2011).
Stanovich, K. E. and R. F. West, "Advancing the Rationality Debate." Behavioral and Brain Sciences, 23(05), (2000): pp. 701-717.

[9] D. Kahneman, P. Slovic and A. Tversky, A. Eds., *Judgment Under Uncertainty: Heuristics and Biases.* Cambridge: Cambridge University Press (1982).



*First Name:

*Last Name:

Middle Initial:

Suffix: --Select--

*Name on Card:

21 characters max.

*Date of Birth: (mm/dd/yyyy) / /

You must be at least 21 years of age to submit an online application.

*SSN: - -

*Email Address:

*Primary Phone Number: - -

*Street Address:

P.O. Box is not accepted.

Street Address 2:

*City:

*State: --Select--

*Zip Code:

*Do you:

○ Rent ○ Own/Buying ○ Other

*Mortgage/Rent: $ .00

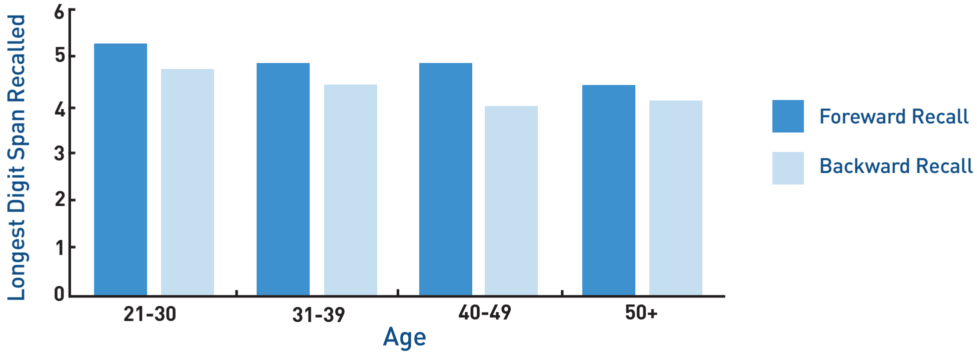
*Time at Address: Year(s)

*Is your mailing address the same as the current home address?

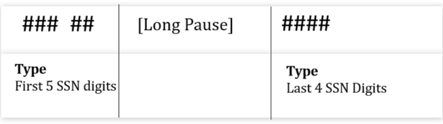
○ Yes ○ No

Short-Term Memory/Digit Span

A digit-span task is used to measure the storage capacity of an individual's short-term or working memory. Adults are able to remember a sequence of 5-7 digits on average. However, these averages decrease with age.[10]



Since fraudsters use short-term/working memory when handling stolen personal info/CC numbers, we can expect them to exhibit slower typing patterns and intervals in longer sequences. BioCatch can detect these patterns, analyze them and determine whether they are suspicious.



### ##	[Long Pause]	####
Type First 5 SSN digits		**Type** Last 4 SSN Digits

The Use of Keyboard Shortcuts

Various studies have established that the use of keyboard shortcuts is faster than standard functions (e.g, toolbar icons), and yet, most users refrain from using such shortcuts. Empirical evidence supports the claim that this is a widespread form of 'satisficing' behavior - due to 'bounded rationality'.[11] Moreover, users do not use shortcuts due to a lack of tech savviness, unawareness of efficiency and unperceived usability.

Since most users exhibit 'satisficing' behavior and a lack of tech savviness in computer applications, these users will use standard functions during a session. Thus, the use of keyboard shortcuts (especially complex shortcuts) can be a good indicator of anomalous behavior and an effective fraud detection parameter.

[10] G. Jones and B. Macken, "Questioning Short-Term Memory and Its Measurement: Why Digit Span Measures Long-Term Associative Learning," *Cognition, 144,* (2015): pp.1-13.

[11] H. A. Simon, *The Sciences of the Artificial* (3rd ed.). Cambridge, U.S: MIT Press (1996); S. Tak, *The Use of Keyboard Shortcuts: Optimizing Versus Satisficing in the Use of Complex Technology.* Graduate Thesis, Eindhoven University of Technology (2007).

Part 2: Fraud Prevention

BioCatch's *Fraud Prevention* capability detects and protects against malware, bots, aggregator and other Remote Access Trojans (RATs). Each of these behave differently than a human being, meaning that they exhibit their own unique behavioral patterns that can be identified. Many of today's remote access attacks originate from humans, using deceptive social engineering methods to trick victims into logging into their own accounts and then taking over.

Asymmetrical Mental Simulations

The *Simulation Heuristic* was identified by Kahneman and Tversky in their studies on heuristics and how they assist individuals in thinking about complex problems with simplified mental operations (1982). They defined the heuristic as "how perceivers tend to substitute 'normal' antecedent events for exceptional ones in psychologically 'undoing' this specific outcome".[12] In other words, a mental strategy where an individual determines the likelihood, the manner in which an event may occur, and/or consequences based upon the ease to mentally picture it.

Mental simulations seem extremely relevant to our discussion, as the way that cyber-criminals mentally image their offensive capabilities may create some asymmetries. Ostensibly, it is easier for them to imagine what they can do to their target, rather than how the other side may react. A capability to harm the other side without being detected could produce a greater sense of omnipotence and invulnerability than is justified, inducing greater risk taking.

In other words, the fraudster's focus on the *Self* may unintentionally obscure thoughts of the *Other*, and producing a false feeling of invulnerability. As a result, the fraudster will exhibit greater risk-taking tendencies.
Based on several attacks detected by our data science team and other empirical data collected from real sessions, fraudsters (social engineering, remote access) unconsciously exhibit more risk-acceptant behavior than typical users. The best example of risk-taking tendencies by fraudsters is repeated attacks on the same website, account or person. In many instances, these attacks are repeated while each time the probability of getting caught increases. Yet, cyber-criminals continue to launch repeated attacks and one could argue that this is a result of asymmetrical mental simulations.

Since cyber-criminals are more prone to risk-taking behavior, their inherent advantage can turn to a weakness as they exhibit abnormal behavior patterns that can be detected by BioCatch.

Network Impatience

Computer scientist Ramesh Sitaraman has asserted that Internet users are impatient and are likely to get more impatient with time.[13] In a large-scale study that was completed in 2012 involving millions of users watching videos on the Internet, Sitaraman showed that users start to abandon online videos if they do not start playing within two seconds. Many commentators have since argued that these results provide a glimpse into the future: as internet services become faster and provide more instant gratification, people become less patient[14] and less able to delay gratification and work towards longer-term rewards.[15]

[12] Kahneman et al., *Judgment Under Uncertainty.*

[13] R. K. Sitaraman, "Network Performance: Does It Really Matter to Users and By How Much?" In *Communication Systems and Networks (COMSNETS), 2013 Fifth International Conference*, (2013): pp. 1-10.

[14] N. G. Carr, "The Patience Deficit", *Edge* (Website), Accessed: 22.8.17, (2014).

[15] C. Muther, C, "Instant Gratification is Making Us Perpetually Impatient". *Boston Globe* (Website), Accessed: 22.8.17, (2013).

Part 3: Continuous Authentication

BioCatch's *Continuous Authentication* capability uses 20 unique features from 500+ behavioral profiling metrics to authenticate a user — without any disruption in the user's experience. The features are selected according to highly-advanced machine learning algorithms, which are employed to maximize the profiling process. After a few minutes of user activity, a robust user profile is built. Once established, the system can detect anomalies and suspicious behavior at an extremely high-level of accuracy and low rate of false positives.

Handedness and Computer Mouse Control

Each handedness group* has performance attributes that are unique to computer mouse movement. When comparing different groups by performance measures like reaction time, time to reach a target, time to click on target and cursory trajectory, the differences become salient.[16] The table below presents the experiment results from Peters & and Ivanoff's study.

Mean Effect Size/Performance	Reaction Time	Transport Time	Targeting Time	Path Deviations
LH/LM		+	+++	+
LH/RM	++		+	+
RH/RM	+		++	+++

***Note:** LH/LM – left-handed/left-hand mouse experience; LH/RM - left-handed/right-hand mouse experience; RH/RM - right-handed/RH mouse experience.

Since each user moves the mouse in a totally unique way, driven by handedness and other motor determinants, this becomes a powerful method of behavioral profiling and detecting anomalies and fraudulent activity.

Conclusion

As mentioned above, researchers and practitioners dealing with behavioral biometrics typically emphasize the computer in computer–human interaction. However, one of the goals of this paper is to present the argument that the human takes precedence over the computer in these interactions and that a deep understanding of online user behavior is key for highly accurate behavioral biometric profiling.

The real power behind behavioral biometrics is that each individual exhibits very unique online behavior that can be profiled and used effectively for authentication and thwarting fraudulent activity. While data science and machine learning provide the necessary means to identify, collect and process extremely large datasets, the core of the profiling process begins with understanding the cyber-psychology that drives user choices, behavior and preferences.

Being able to capture these patterns is what makes behavioral biometrics the most advanced technology in today's marketplace for continuous authentication, identity proofing and fraud prevention.

[16] M. Peters and J. Ivanoff, "Performance Asymmetries in Computer Mouse Control of Right-Handers, and Left-Handers with Left-and Right-Handed Mouse Experience." *Journal of Motor Behavior*, 31(1), (1999): pp.86-94.

References

Ahmed, A.A.E. and Traore, I. “Detecting Computer Intrusions Using Behavioral Biometrics”. In *PST* (2005).

Bailey, K.O., Okolica, J.S. and Peterson, G.L. “User Identification and Authentication Using Multi-Modal Behavioral Biometrics.” *Computers & Security, 43*, (2014): pp. 77-89.

Bo, C., Zhang, L., Jung, T., Han, J., Li, X.Y. and Wang, Y. “Continuous User Identification via Touch and Movement Behavioral Biometrics.” In *Performance Computing and Communications Conference (IPCCC), 2014 IEEE International*, (2014): pp. 1-8.

Bo, C., Zhang, L., Li, X.Y., Huang, Q. and Wang, Y. “Silentsense: Silent User Identification via Touch and Movement Behavioral Biometrics.” In *Proceedings of the 19th Annual International Conference on Mobile Computing & Networking*, (2013): pp. 187-190.

Carr, N. G, “The Patience Deficit”, *Edge* (Website), Accessed: 22.8.17, (2014).

Deutschmann, I., Nordström, P. and Nilsson, L. “Continuous Authentication Using Behavioral Biometrics.” *IT Professional*, 15(4), (2013): pp.12-15.

Evans, J. & Frankish, K. eds., *Two Minds: Dual Processes and Beyond*. Oxford: Oxford University Press, 2009.

Evans, J. “Dual-Processing Accounts of Reasoning, Judgment, and Social Cognition.” *Annual Review of Psychology*, 59, (2008): pp. 255-278.

Jones, G. and Macken, B. “Questioning Short-Term Memory and Its Measurement: Why Digit Span Measures Long-Term Associative Learning.” *Cognition*, 144, (2015): pp.1-13.

Kahneman, D. *Thinking, Fast and Slow*. New York: Farrar, Straus and Giroux, 2011.

Kahneman, D. Slovic, P. & Tversky, A. Eds., *Judgment Under Uncertainty: Heuristics and Biases*. Cambridge: Cambridge University Press, 1982.

Moskovitch, R., Feher, C., Messerman, A., Kirschnick, N., Mustafic, T., Camtepe, A., Lohlein, B., Heister, U., Moller, S., Rokach, L. and Elovici, Y. “Identity Theft, Computers and Behavioral Biometrics. In *Intelligence and Security Informatics, 2009. ISI´09. IEEE International Conference*, (2009): pp. 155-160.

Muther, C. “Instant Gratification is Making Us Perpetually Impatient”. *Boston Globe* (Website), Accessed: 22.8.17, 2013.

Norman, K. L. *Cyberpsychology: An introduction to human-computer interaction* (Vol. 1). New York, NY: Cambridge University Press, 2008.

Peters, M. and Ivanoff, J. “Performance Asymmetries in Computer Mouse Control of Right-Handers, and Left-Handers with Left-and Right-Handed Mouse Experience.” *Journal of Motor Behavior, 31*(1), (1999): pp. 86-94.

Saevanee, H. and Bhatarakosol, P. “User Authentication Using Combination of Behavioral Biometrics Over the Touchpad Acting Like Touch Screen of Mobile Device”. In *Computer and Electrical Engineering, 2008. ICCEE 2008. International Conference*, (2008): pp. 82-86.

Simon, H. A. *The Sciences of the Artificial* (3rd ed.). Cambridge, U.S: MIT Press, 1996.

Sitaraman, R.K. “Network Performance: Does It Really Matter to Users and By How Much?” In *Communication Systems and Networks (COMSNETS), 2013 Fifth International Conference*, (2013): pp. 1-10.

Stanovich, K. E. & West, R. F. “Advancing the Rationality Debate.” *Behavioral and Brain Sciences, 23*(05), (2000): pp. 701-717.

Tak, S. *The Use of Keyboard Shortcuts: Optimizing Versus Satisficing in the Use of Complex Technology*. Graduate Thesis, Eindhoven University of Technology, 2007.

Wang, L. ed., *Behavioral Biometrics for Human Identification: Intelligent Applications: Intelligent Applications*. IGI Global, 2009.

About BioCatch

BioCatch is a cybersecurity company that delivers behavioral biometrics, analyzing human-device interactions to protect users and data. With an unparalleled patent portfolio and deployments at major banks around the world that cover tens of millions of users to date, BioCatch has established itself as the industry leader. For more information, please visit www.biocatch.com.