Tailored Cybersecurity Interventions

Hein Rödel
University of Twente
P.O. Box 217, 7500AE Enschede
The Netherlands
h.a.rodel-1@student.utwente.nl

ABSTRACT

In cybersecurity, there are different ways you have to protect yourself against attacks. One of these ways is the attack wherein the vulnerable party is a person and not a system These attacks are made possible due to human engineering. To prevent this kind of attacks there are cybersecurity interventions to learn people how to not fall for these attacks. These pieces of training are however far from perfect and do not appeal to one as much as to the other. This paper aims to define groups of people as well as situations wherein for which the cybersecurity intervention can be tailored. By doing literature research multiple socio-demographic and personality traits have been identified, as well as parts of interventions. It is found that there are two groups within socio-demographics and two groups within personalities that are easily identifiable that profit from a different kind of cybersecurity intervention than another found group. These groups have been translated into the found characteristics of the cybersecurity interventions. Next to that, the learning characteristics have been combined with learning objectives found in human behaviour models.

Keywords

Cybersecurity, intervention, tailored, socio-demographics, personality traits, health belief model, theory of planned behaviour, Phishing.

1. INTRODUCTION

The number of cyber-attacks is high and increasing, the cost for these attacks has grown [1]. Also, since the amount of data that is being leaked is becoming more. Human engineering is part of the top 5 of most common causes for data breaches. In cybersecurity human engineering translates into actions that encourage people to perform a certain action or give away confidential information. A well-known example of human engineering is Phishing, yet it may be as simple as placing a phone call while impersonating someone to gain access to information [2]. This may seem like a tiresome way, yet it is easier and cheaper than a brute force attack [3].

To prevent this kind of attack people have to be trained to identify these attempts of human engineering and take the right precautions once the thread has been identified. There are several solutions to get training since there are multiple companies that have created such a training [4].

One of those ways is to get training from the company you work at. There has been some research on what kind of elements within a training are effective. This research has evaluated these elements on the whole group that was part of the study. Yet nobody is the same and as such not everybody learns in the same way [5][6].

To make the training more effective a tailored intervention within a company may be needed to increase the effectiveness of the intervention. Based on standing research on interventions, characteristics of the intervention may be more or less effective on certain groups of a population [7]. To find out what groups of the population respond differently to certain characteristics literature research is going to be performed.

All of these different traits people have are can be assessed to find out what learning style fits with the personality. Learning styles can however be assessed in a lot of different ways.

In language learning strategies there are several frameworks that work slightly different one of them is made by Oxford. This framework makes a big difference in Direct and Indirect Strategies. Direct strategies are the strategies that are directly involved in learning. The 3 categories that are included are Memory, Cognitive, and Compensation strategy. These categories make sure that the language is learnt and repeated, this can all be done on your own. The Indirect strategies are divided into metacognitive strategies, Affective strategies and social strategies. These involve planning asking questions and motivating yourself to learn. The direct and indirect strategies are also referred to as cognitive and metacognitive strategies when referred to by other frameworks [9].

Next to strategies there are some differences in learning styles. The first model to discuss is the VARK model. VARK stands for Visual, Auditory, Read/Write and Kinaesthetic learners.

- Visual learners (V): People that have the easiest time learning when the information is presented in the form of symbols. Graphs, flow charts and other forms of visual information work best for visual people;
- Auditory learners(A): People that prefer to get their information by hearing it. This is by forms of presentation or a video;
- Read/Write learners(R): people who like to learn using written text. This is not limited to what is written in a book but also extends to for example the handouts of a PowerPoint presentation;
- And lastly the Kinaesthetic learners(K): these are the people that learn by doing [24].

Next to this, there is still Kolb's learning style interventions Kolb splits learning into 4 repetitive parts. Concrete experience also known as feeling, Reflective Observation known as watching, Abstract Conceptualisation also known as thinking and lastly Active Experimentation also known as Doing. Once these concepts are known there are a few styles that people normally have.

- Converger: The converger is great in the areas of Abstract Conceptualization and active experimentation;
- Diverger: For divergers learning works best when focussing on concrete Experience and Reflective Observation;
- Assimilator: These people learn best when focussing on Abstract conceptualization and reflective Observation;
- Accommodator: These people like learning in the areas of concrete experience and active experimentation [14].

Next, there is the reason someone would want to learn something. For this, two models are going to be used in this paper.
Firstly there is the model of planned behaviour. The theory of planned behaviour has 3 main concepts on which it stands:

- Attitude toward the behaviour: This states the view that a person has towards the problem at hand and how this should be handled;
- Subjective norm: The view of significant others, like parents teachers or friends, that influence the attitude of a person towards the subject;
- Perceived behavioural control: The amount of control the person has in learning or doing what is required toward the subject.

These three base principles converge toward the intent of learning or doing what is required for the subject. This intent is combined with the actual control someone has on learning or doing the subject which results in the behaviour of the person [8].
The other model that is going to be used is the health belief model. This model was created to explain behaviour around choices around one's health yet can be extrapolated toward other fields of study. This model stands on a few theoretical constructs:

- Perceived susceptibility: This refers to the chance someone will have to handle the given subject;
- Perceived severity: This indicates the amount of influence the subject will invoke on the life of the person;
- Perceived benefits: This gives the number of benefits one thinks when doing something about the subject;
- Perceived barriers: What stands in the way of learning or doing what is needed not to be influenced by the subject;
- Modifying variables: This includes the demographic(age, sex, race), psychosocial(personality, social class) and structural variables(what is already known on the subject). This mostly influences the previous variables;
- Cues to action: Some kind of stimulus, internal or external, that gives an extra nudge toward dealing with the subject;
- Self-efficacy: This indicates one's own belief of being able to solve or deal with the subject [16].

Lastly, there are personality traits. For personality the Big 5. This grouping is done using the following categories:

- Openness: These people are open to experience and are intellectually curious. These people tend to be more creative;
- Conscientiousness: This relates to self-discipline high on this scale often translates to focussed while low on this scale is being interpreted as spontaneity or being sloppy;
- Extraversion: The amount of interaction with the world, extravert people are often related to as full of energy;
- Agreeableness: This is the tendency to get along with people, these people are often referred to as generous and helpful;
- Neuroticism: This is the tendency to show emotions, people high on this scale seem emotionally unstable.

In all of these categories, one gets a score higher or lower is not better but indicates where you are in the spectrum [4].

1.2 RELATED WORK

A literature search has been performed using Scopus and google scholar as sources. The initial combination of words: 'tailored cybersecurity interventions' yielded 1 result. This result is focussed completely on cybersecurity on social networks, in this case, Facebook[10]. A search using the words 'tailored cybersecurity' was used. This resulted in 69 documents. The results varied but most of the results included security by design, reinforcement learning or a framework for cybersecurity. Also, a search using the words 'cybersecurity interventions' was performed. The results for this search led to the way learning is done, for example by gamification, and other results yet not answering this question.

However, there is quite some research based on socio-demographic traits. Male and female students do for example prefer different ways of learning [21][11]. Also, age has a role in the learning strategies of people [20][2]. These differences become especially important when doing this training in a digital or online environment.

Next to the socio-demographic traits, one can look at behavioural models, a good start will be the Theory of planned behaviour[12] or the Health belief model[16]. The scope of this research is based on the perceived benefits and barriers of the trainee. Both of these characteristics are used to create a prediction on how the trainee will perform. These models also describe ways to modify these variables to positively change the attitude towards the problem.

One can then look at personality traits. People that are extravert also tend to prefer different styles of teaching than introverted people. The paper of Z. Yu [23] shows that there is a difference in learning for different genders, ages and level of education. Next to this, there is research on how to make tailored advertisements. This includes working with the big 5 personality dimensions[8]. Since these personality traits are somewhat harder to determine than for example the sex of a person, these results have to be gathered by the use of a survey.

1.3 PROBLEM STATEMENT

Cybersecurity interventions are well structured but not well researched. The research that has been done shows that the better the research the lower the result of the intervention[3]. To increase the effectiveness of these interventions a tailored approach of the intervention may be desired.

1.3.1 RESEARCH QUESTION

To create tailored interventions 2 questions need to be answered.

Q1: Can standardised groups be identified that need to be addressed in tailored cybersecurity interventions?

This question has two sub-questions:

Q1.1: Can standardized groups be determined based on the socio-demographic characteristics of a person? and, Q1.2: Can standardized groups be determined based on a survey?

These 2 questions are separated since they both give information about the person, yet the information has a completely different basis and thus should be handled differently. Once standardized groups have been identified this will be implemented into the following question:

Q2: What characteristics of a cybersecurity intervention should be implemented for what groups?

2. METHODOLOGY

To lay groundworks for this problem research has to be performed in other areas. Firstly, a search will be performed to find out if there are similar problems in other fields. If this is not the case the answer will be sought in human psychology. If a search based on psychology needs to be performed at the start of this search will be:

- Socio-demographics traits of a person, for example:
  - Age;
  - Gender.
- Based on a survey, for example:
  - Personality (NEO PI-R) traits[4];
  - Theory of planned behaviour[12];
  - Health belief model[16].

Based on the research a list of properties will be created. This list will contain properties that may influence the ability of people to learn how to prevent human engineering in the sense of cybersecurity. Once the properties of the person are known the intervention characteristics as described in [3] will be analysed. Once these are known an in-depth literature search will be performed to find more information on the intentions of the different parts of the intervention. This is done to get a better understanding of the underlying psychological workings of the interventions.

Based on this literature search an attempt will be made to make a connection between personality traits and certain components of cybersecurity interventions.

Once this trade is made Phishing interventions will be highlighted and put into context in relation to the health belief model.

3. RESULTS

This paper will take into account a few different sociodemographic properties continued by the personality of a person. After these traits, the results will continue with known cybersecurity training and the interaction with the theory of planned behaviour and the Health belief model.

3.1 SOCIO-DEMOGRAPHIC TRAITS

Based upon simple questions a lot of information can come to light when learning something. These simple questions pose a good option to make learning more effective for each group of the training. The socio-demographic traits that will be taken into account are age and sex

3.1.1 AGE

In age, there are differences in groups. But the ages of the groups vary in most studies. Besides that the groups that involve children are mostly build-up based on their knowledge level giving some indication on age. This is done for example in the paper of Joel Mokuedi Magogwe and Rhonda Oliver. In this paper, there are 3 groups defined. These groups generalized 11-15 (group 1), 16-20 (group 2) and 16-25(group 3). These are based upon primary secondary and tertiary education. This paper shows that there Is a shift in learning strategies from social learning toward metacognitive learning starting at group 1 and going toward the 3rd group. This indicates a changing learning style between the ages of 11 and 25 [13].

However looking at higher ages it is visible that, when looking at distance learning, there is still a slight increase in learning strategies. It is found by P. M. Z. Alliprandini et al. that people between the age of 18-35 still increase in strategy. Once the age of 35 is reached there is no increase in strategy anymore and the level of learning stays the same. This however is only a change in learning strategy and not learning style. This show for example a better rhythm in planning over time [1].

These results tell that there is an increase in learning strategies over age. This increase is still in place when someone enters the working class in the ages between 18 and 35. However, this is an increase in the strategy of people when working from home. Since this change mainly involves an increase in metacognitive learning this does not fit very well with cybersecurity interventions since these usually can be done within 15 minutes [18].

3.1.2 SEX

Next, there are some differences in Sex. Male and Female people do learn differently and the way of teaching has to be adapted to that [15].

The first difference in learning between men and woman is the number of different styles they prefer. Based upon the VARK model most females prefer a single learning style. The style that woman like are mostly by mode K, this implies that woman learns by doing, the second most common mode is R, this

means by reading and writing about it. Men on the other hand prefer a combination of learning styles [21].

When looking at multiple ways of learning for a certain topic most males will prefer all ways of information in this method. This means getting information by visual, auditory, read/write and by doing. When looking at multiple ways next to all four males like it best to get a combination of visual information and by doing [21].

Next, there is research, with students, on the scale of Kolb. This gives some indication of the learning styles people prefer. In a study by Garland and Martin, it is shown that for females there is no significant difference in learning styles. For females, there is however a strong correlation to Reflective observation and a strong negative correlation to abstract conceptualisation.

For males, there is a significant correlation between the communication part of the study and Abstract conceptualisation. However, regarding the main content, there is a slightly lower correlation. Regarding the main content male student did not show a significant yet strong correlation toward concrete experience [7].

Next to these general differences within student groups, there is also research done based on language learning. Research done by Jamiah, Mahmud, Muhayyang, shows that females prefer a social approach to learning whereas males prefer having fun and a more logical approach to learning a language. Translated to the Oxford learning modes this translates for a top 2 for males of preference with on one compensation and at number 2 cognitive. For females, these were also high and in the same order yet number one was social. This shows that for females there needs to be more interaction and doing however since this study is solely based upon language learning it is not clear if this fully translates to learning in the context of cybersecurity [11].

3.2 PERSONALITY

The personality of a person may influence the way this person learns. Some papers focus on a specific point of the big 5 personality index. Also, some studies keep all the 5 dimensions of the big 5 into account. It is shown that there is a relation between conscientiousness, openness and agreeableness and the cognitive and metacognitive functions [17].
Also, it is shown by the British psychology society that there is a correlation between neuroticism and surface processing as well as conscientiousness. However, openness has a negative correlation with surface processing. This shows that people that rate high on the neuroticism or conscientiousness scale do well with getting all the information before starting to learn, these people learn for example by learning all the facts. People that rate high on the openness scale however do not like this way of learning. Any other kind of learning is fine for them [5].

3.3 WELL KNOWN INTERVENTIONS

There are a lot of different interventions that are made. For the sake of simplicity, this paper is limited to phishing. Within the world of phishing, some well-known interventions have different ways of learning people how to work cope with the given situation. There are 3 ways of doing so specified in this paper. The first way in this paper is made by several institutions and is mainly by telling people in words in the form of a document. In this paper the read should take about 15 minutes

The second is by playing a game: ‘anti-phishing Phil’ for about 8 minutes or reading a strip ‘phishGuru’ for about half a minute. All of these ways of improvement were tested by sending real e-mails and phishing e-mails. In this study, it is shown that the longest study showed the best result. Yet the other 2 ways also showed a big improvement in the study. The different ways of presenting the information does open a possibility for improvement. All of these pieces of training choose to show you how to find what is phishing and what are real emails from a reliable source. This relies on the assumption that people are willing to not click on a link in a phishing e-mail. From a base instinct, people want to avoid getting caught by phishing [19].

3.4 BEHAVIOURAL MODELS

The willingness to spend time to avoid getting caught by phishing can influence the expected outcome of the attempt of phishing. To change the willingness of people the same learning styles can be used, but the information needs to be different. When the willingness of spending the time is not high enough the chance of not clicking becomes very low. This can be explained by the health belief model [12].
The health belief model states that eight variables influence people to avoid risks for their health. These variables are their perceived susceptibility, severity, benefits and barriers. Also, this contains other modifying variables cues to action and their self-efficacy. When there is a discrepancy between one of the variables and the real values people tend to get an unrealistic portrait of the truth colouring them into taking non-beneficial actions [8]. For Phishing the most to gain is on the front of the perceived benefits. For the perceived benefits, it may already be sufficient if an IT department sends a monthly e-mail stating what risks there are and how to work with those [18].

4. CONCLUSION

There are multiple ways to group people that prefer different kinds of learning. These different kinds of ways of grouping give an answer to Q1.

Sex:

- Males prefer multiple ways of information that give information preferably by showing the information. A male then needs to reflect on the concepts that were at hand to learn best;
- - Females prefer to learn by doing to get the experience of what happens and then reflect on what happened to get the best way of learning.

Personality:

- People that score high on the Neurotisist and Conscientiousness scale prefer to get all the information and make sure to know all the ins and outs;
- People that score high on the Openness scale prefer opposite and like to the point information.

However, there is literature that tells us that the learning strategies of people increase until they are around 35 years old this does not have an implication concerning the cybersecurity intervention. A cybersecurity intervention is not a long learning process, not when addressing for example Phishing.

	Male	Female
Neurotisist	Giving all information based upon visual input	Getting all information and then by doing it a to find out right from wrong
Conscientiousness	Giving all information based upon visual input	Getting all information and then by doing it finding out what goes right and what goes wrong
Openness	Giving information while sticking to the point in a visual way	Giving them to the point information and then by doing it finding out what goes right or wrong

Table 1: ways to get information

When looking at what ways may or may not be useful a comic may be more useful to male persons that have a very open character. If the male has more neuroticism and Conscientious characteristic the way of giving information may be varied to a small movie since this can give a lot more information to work with. Whatever way of giving information will be given needs to take into account to give the concepts of phishing and show the bigger picture. Females need to experience to learn. A good way would be information with a lot of examples of how to avoid getting caught by phishing. For this also a video would be good. However, for females, the concepts do not give the whole picture and the examples need to be more concrete. Lastly, the willingness of people can be taken into account this would be done by the same methods however the message needs to show a cue to action or another way to increase the perceived severity or susceptibility of a phishing attack.

For future research, the data gathered in this paper could be set into perspective by doing experiments with it. For this, a survey still needs to be made to get all the needed information to make give this person the right training. Once this data is gathered an experiment can be done with a control group as it would normally be done and a group that uses the relations found in this paper. For this experiment one could use the following setup:
In the paper there are 3 ways described for interventions on Phishing.

1. Giving all information by means of reading several pages of text and visuals. This text gives all the information regarding the different approaches and several examples of phishing.
2. A game ‘ani-Phishing Phil’ that learns people by doing what to do with Phishing and how to recognise it.
3. Phish-guru, a small strip that quickly triggers people to think about the implications of Phishing.

	Male	Female
Neurotisist or Conscientiousness	1	A combination of 1 and 2
openness	3	Only 2 would suffice

Table 2: applied ways to get information

To implement the models concerning the willingness of people can be could be to examine the differences between regular stimulants and no stimulants. This would, according to the literature yield the result with the best improvement.
For practitioners, there is something else to get from this paper. For practitioners this information would be best put to use starting at the belief models. In the health belief model there are 4 basic constructs on which employees would be more susceptible to for example Phishing. Based upon these constructs the following actions could be taken when dealing with Phishing.

- Low on perceived susceptibility: In this case the employee does not feel that he/she is no threat to Phishing, the training should contain at least a good amount of training that shows how everybody is susceptible to phishing;
- Low on perceived severity: This training should at least cover some information on what a phishing leak can lead to and what monetary losses there are connected to cybercrime based on Phishing;
- Low on perceived benefits: As shown by Schymik and Du the perceived benefits can be stimulated by a more detailed discussion or going through case studies but can also be stimulated by sending regular e-mails containing the costs faced by cybersecurity threads;
- Low perceived barriers: In this case employees do not know what to prevent Phishing, or what they have to do is too much effort. Employees need to be educated on what they can do about phishing.

The other 3 constructs that finish the health belief model have been added later to fill gaps in the theory and all have an influence on one of the above constructs.
Once the discrepancy has been established together with the extra needed information the way of presenting that information to the employee can be found in table 2 if it concerns Phishing. If a cybersecurity thread is chosen other than Phishing one can find the more generalized information in table 1.

5. DISCUSSION

This paper links different ways of learning to different kinds of personality. However, of all the results that have been found that create this paper use different groups of people. Some studies work with the class of people where this paper is aimed toward. Yet, there are also a lot of papers that have worked with students. Students do not represent the population of the earth as a whole. For example, the IQ of students is higher than the average IQ of the working class. This may influence the way that people learn [6].

Next, there is age, where there is little change in learning styles or strategies there is a significant difference in learning speed. Older people can learn as much as younger people, however, they do use more time to get to the same level. This implies that, in the case of cybersecurity interventions, more follow-up should be done. Also, when giving the same intervention, even though the learning method is right, not the same result should be expected [22].

ACKNOWLEDGEMENTS

I would like to thank Jan-Willem Bullee. Due to his insights in the matter the paper has gotten the view it has taken on. Next to that, for all the questions that arose during the last ten weeks regarding research or writing of papers.

REFERENCES

[1] P. M. Z. Alliprandini, M. A. Pavesi, D. Vicentini, and J. T. Sekitani, "Guidance on the use of learning strategies in distance education (DE) as a function of age and gender," *Int. J. Inf. Commun. Technol. Educ.*, vol. 11, no. 3, pp. 53–61, 2015, doi: https://doi.org/10.4018/IJICTE.2015070105.

[2] S. Bastable, "Age-Specific Learning Characteristics," *Nurse as Educ.*, pp. 94–98, 1997.

[3] J. W. Bullee and M. Junger, "How effective are social engineering interventions? A meta-analysis," *Inf. Comput. Secur.*, vol. 28, no. 5, pp. 801–830, 2020, doi: https://doi.org/10.1108/ICS-07-2019-0078.

[4] P. T. Costa and R. R. McCrae, *The revised NEO personality inventory (NEO-PI-R)*, no. January 2008. 2008. doi: https://doi.org/10.4135/9781849200479.n9.

[5] V. Donche, S. De Maeyer, L. Coertjens, T. Van Daal, and P. Van Petegem, "Differential use of learning strategies in first-year higher education: The impact of personality, academic motivation, and teaching strategies," *Br. J. Educ. Psychol.*, vol. 83, no. 2, pp. 238–251, 2013, doi: https://doi.org/10.1111/bjep.12016.

[6] S. Fischbein, "IQ and social class," *Intelligence*, vol. 4, no. 1, pp. 51–63, 1980, doi: https://doi.org/10.1016/0160-2896(80)90006-9.

[7] D. Garland and B. N. Martin, "Do gender and learning style play a role in how online courses should be designed?," *J. Interact. Online Learn.*, vol. 4, no. 2, pp. 67–81, 2005.

[8] L. Goldberg, "An alternative 'description of personality': the big-five factor structure.," *J. Pers. Soc. Psychol.*, vol. 59 6, pp. 1216–1229, 1990.

[9] A. A. Hardan, "Language Learning Strategies: A General Overview," *Procedia - Soc. Behav. Sci.*, vol. 106, pp. 1712–1726, 2013, doi: https://doi.org/10.1016/j.sbspro.2013.12.194.

[10] E. Ikhalia, A. Serrano, D. Bell, and P. Louvieris, "Online social network security awareness: mass interpersonal persuasion using a Facebook app," *Inf. Technol. People*, vol. 32, no. 5, pp. 1276–1300, 2019, doi: https://doi.org/10.1108/ITP-06-2018-0278.

[11] J. Jamiah, M. Mahmud, and M. Muhayyang, "Do Male and Female Students Learn Differently?," *ELT Worldw. J. English Lang. Teach.*, vol. 2, no. 2, p. 110, 2016, doi: https://doi.org/10.26858/eltww.v2i2.1691.

[12] M. P. H. Kan and L. R. Fabrigar, "Theory of Planned Behavior," in *Encyclopedia of Personality and Individual Differences*, V. Zeigler-Hill and T. K. Shackelford, Eds. Cham: Springer International Publishing, 2017, pp. 1–8. doi: https://doi.org/10.1007/978-3-319-28099-8_1191-1.

[13] J. M. Magogwe and R. Oliver, "The relationship between language learning strategies, proficiency, age and self-efficacy beliefs: A study of language learners in Botswana," *System*, vol. 35, no. 3, pp. 338–352, 2007, doi: https://doi.org/10.1016/j.system.2007.01.003.

[14] S. McLeod, "Learning KOLB," 2017. https://www.simplypsychology.org/learning-kolb.html

[15] M. Philbin, E. Meier, S. Huffman, and P. Boverie, "A survey of gender and learning styles," *Sex Roles*, vol. 32, no. 7–8, pp. 485–494, 1995, doi: https://doi.org/10.1007/BF01544184.

[16] I. M. Rosenstock, "Historical origins of the health belief model. Health Education Monographs," *Health Educ. Monogr.*, vol. 2, no. 4, pp. 328–335, 1974, doi: http://dx.doi.org/10.1177/109019817400200403.

[17] S. Ruffing, E. Hahn, F. M. Spinath, R. Brünken, and J. Karbach, "Predicting students' learning strategies: The contribution of chronotype over personality," *Pers. Individ. Dif.*, vol. 85, pp. 199–204, 2015, doi: https://doi.org/10.1016/j.paid.2015.04.048.

[18] G. Schymik and J. Du, "Student Intentions and Behaviors Related to Email Security: An Application of the Health Belief Model," *Proc. Conf. Inf. Syst. Appl. Res.*, 2017, [Online]. Available: http://iscap.info

[19] S. Sheng, M. Holbrook, P. Kumaraguru, L. F. Cranor, and J. Downs, "Who falls for phish?," p. 373, 2010, doi: 1https://doi.org/0.1145/1753326.1753383.

[20] J. L. Wahlheim, C. N., McDaniel, M. A., & Little, "Category Learning Strategies in Younger and Older Adults: Rule Abstraction and Memorization," *Physiol. Behav.*, vol. 176, no. 5, pp. 139–148, 2018, doi: https://doi.org/10.1037/pag0000083.Category.

[21] E. A. Wehrwein, H. L. Lujan, and S. E. DiCarlo, "Gender differences in learning style preferences among undergraduate physiology students," *Am. J. Physiol. - Adv. Physiol. Educ.*, vol. 31, no. 2, pp. 153–157, 2007, doi: https://doi.org/10.1152/advan.00060.2006.

[22] T. N. Welsh, L. Higgins, and D. Elliott, "Are there age-related differences in learning to optimize speed, accuracy, and energy expenditure?," *Hum. Mov. Sci.*, vol. 26, no. 6, pp. 892–912, 2007, doi: https://doi.org/10.1016/j.humov.2007.04.004.

[23] Z. Yu, "The effects of gender, educational level, and personality on online learning outcomes during the COVID-19 pandemic," *Int. J. Educ. Technol. High. Educ.*, vol. 18, no. 1, Dec. 2021, doi: https://doi.org/0.1186/s41239-021-00252-3.

[24] "4 Different learning styles you should know: the VARK model."

https://educationonline.ku.edu/community/4-different-learning-styles-to-know (accessed Jun. 03, 2021).