Student: 2061187

**Self-Efficacy in Information Security**

# What is self-efficacy in information security?

(Ozer & Bandura, 1990) Simply explains that self-efficacy is the way in which people believe to be able to use their skills to promote motivation and cause action to gain control of events. There are theories that self-efficacy is one of the most important factors in humans that change our behaviours (Bandura & Jourden, 1991).

Self-efficacy directly affects tasks that one tries to complete when self-efficacy is high motivation, effort and willingness is higher. This in turn increases one’s chances of succuss within the given environment (Hartzel K, 2003). In this case information security will be the environment being affected.

This makes self-efficacy very important in information security when dealing with attacks such as spyware and social engineering. Self-efficacy makes one believe in the ability to protect their assets from malicious attacks (Rhee et al, 2009, p1).

Self-efficacy could impact information security in different ways which are; higher self-efficacy causes people to be more conscious about security, higher self-efficacy causes people to have stronger intentions to improve security and successful security attacks lower one’s self-efficacy (Rhee et al, 2009, p2.2).

In this review the scope will be looking at how self-efficacy can impact information security and impacts, risks, and improvements we could make to it.

# Impact on end users

Generally higher self-efficacy means people have better information security which does the reverse for those with lower self-efficacy. Lower self-efficacy directly affects two types of security attacks making them much easier to successful gain assets these are; Social Engineering and Spyware attacks.

Social engineering can be made easier by low self-efficacy, this is because they tend to be less conscious on threats. (Krombholz K et al, 2015) This means that attackers find it easier to manipulate them for information assets exploiting people/companies and showing vulnerabilities in security.

The impact social engineering can have on end users is dependent on how big the breach is, they can cause billions of pounds to companies, but end users also have substantial induvial impacts (Workman M, 2007). These impacts cause customers to lose valuable/personal assets, meaning that they can be vulnerable to more threats such as identify theft and loss of control over other personal assets such as their email (Workman M, 2007).

Spyware also is made easier by low self-efficacy; this is because being less conscious on threats means that end users are more likely to install spyware hidden as other data. Impacts of spyware tend to be more on the end-user because they are more targeted towards those who have lower self-efficacy and less information security knowledge.

Spyware commonly is malicious code that sits within the end-user’s system taking information and sending it back to the hacker. 80% of computers have spyware currently installed onto their systems, this is a very high percentage where self-efficacy has come into play. This means that a keylogger could send passwords back to hackers and go undetected since the end user is less information security aware (Moshchuk A et al, 2006, p1).

# Security risks for companies

Research has shown that owners that do not give sustainable budgets for information security, have more security risks within the business. This can be down to self-efficacy, owners that do not understand information security as well tend to give lower budgets (Soomro Z. A. et al, 2016).

Companies are more likely to receive social engineering attacks due to the large amount of support that can be contacted. This means that people pose as others to gain access into their accounts, this can lead to multiple accounts being breached normally through password resetting using Gmail accounts.

The risks these propose for companies is high because, lower budgets mean that they cannot protect assets as well. The low self-efficacy can teach others that security doesn’t matter therefore replicating this low self-efficacy.

# How it can be improved

To improve self-efficacy spreading awareness is the most preferred method, however shared language did not influence either the intention or attitude to share knowledge. (Tamjidyamcholo et al, 2013) Therefore more ways need to be introduced to improve self-efficacy to be able to in turn improve information security.

Improving self-efficacy will reduce the threats of many security risks majorly social engineering and spyware. To be able to address these issues within information security we need to start from the source which is improving self-efficacy within oneself.

To improve induvial self-efficacy within information security we can set small tasks to complete within security and show how these controls are helping to defend our assets. Once they can see that they can improve security, see it working and understand why we need the security, their own self-efficacy will start to improve (Bandura A, 2006).

(Margolis H & McCabe P. P, 2006) Shows one of the most proven ways to improve self-efficacy within social groups is role/peer modelling. This means setting an employee with high self-efficacy a targeted task. The low self-efficacy can watch over and observe how they complete this task, this maximum the observer’s chance to absorb a want to improve. Self-efficacy tends to be improved in this method because we need to show individuals that they can effectively work therefore sparking self-belief in themselves.

# Conclusion

In conclusion self-efficacy is one of the defining features within information security, it subconsciously affects an individual’s cyber security. This means on a personal level and business asset protection is affected because some may not as vigilant and motivated to go out of their way to help better secure data.

(Rhee et al, 2009) helps to conclude that self-efficacy in information security is a defining aspect and should be considered more widely. It is a serious topic that causes many human errors daily therefore breaches within information security comprising assets.

Research has shown that self-efficacy has many flaws that need to be improved, it is hard to develop methods to enhance self-efficacy since it is psychological. As technology advances, we may find we are able to better identify self-efficacy and improve it.

**References**

Bandura, A., & Jourden, F. J. (1991). Self-regulatory mechanisms governing the impact of social comparison on complex decision making. *Journal of personality and social psychology*, *60*(6), 941. <https://psycnet.apa.org/record/1991-28996-001>

Bandura, A. (2006). Guide for constructing self-efficacy scales. *Self-efficacy beliefs of adolescents*, *5*(1), 307-337.  
<https://books.google.com/books?hl=en&lr=&id=P_onDwAAQBAJ&oi=fnd&pg=PA307&dq=improve+my+own+self+efficacy&ots=rjMLp2EfyS&sig=zyyYgcS974waSrCHWRlgRb5XsTg>

Hartzel, K. (2003). How self-efficacy and gender issues affect software adoption and use. *Communications of the ACM*, *46*(9), 167-171.   
<https://dl.acm.org/doi/pdf/10.1145/903893.903933>

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. *Journal of Information Security and applications*, *22*, 113-122. <https://www.sciencedirect.com/science/article/pii/S2214212614001343>

Margolis, H., & McCabe, P. P. (2006). Improving self-efficacy and motivation: What to do, what to say. *Intervention in school and clinic*, *41*(4), 218-227. <https://journals.sagepub.com/doi/abs/10.1177/10534512060410040401>

Moshchuk, A., Bragin, T., Gribble, S. D., & Levy, H. M. (2006). A Crawler-based Study of Spyware in the Web. In *NDSS* (Vol. 1, p. 2). <http://courses.cs.washington.edu/courses/cse454/15wi/papers/spycrawler.pdf>

Ozer, E. M., & Bandura, A. (1990). Mechanisms governing empowerment effects: a self-efficacy analysis. *Journal of personality and social psychology*, *58*(3), 472. <https://psycnet.apa.org/doiLanding?doi=10.1037/0022-3514.58.3.472>

Rhee, H. S., Kim, C., & Ryu, Y. U. (2009). Self-efficacy in information security: Its influence on end users' information security practice behaviour. *Computers & security*, *28*(8), 816-826. <https://www.sciencedirect.com/science/article/pii/S016740480900056X>

Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management*, *36*(2), 215-225. <https://www.sciencedirect.com/science/article/pii/S0268401215001103>

Tamjidyamcholo, A., Baba, M. S. B., Tamjid, H., & Gholipour, R. (2013). Information security–Professional perceptions of knowledge-sharing intention under self-efficacy, trust, reciprocity, and shared-language. *Computers & Education*, *68*, 223-232. <https://www.sciencedirect.com/science/article/pii/S0360131513001310>

Workman, M. (2007). Gaining access with social engineering: An empirical study of the threat. *Information Systems Security*, *16*(6), 315-331. <https://www.tandfonline.com/doi/abs/10.1080/10658980701788165>