SAFE

REDUCE THE HUMAN RISK IN CYBERSECURITY

Secura
A BUREAU VERITAS COMPANY

Fortunately, we have seen growing attention for the human side of information security in recent years. The penny has dropped; we are not yet completely safe with attention to technology and processes only. What needs to be done to make employees as resilient as possible? People are complex, not one-dimensional and behavior is driven by various factors. In order to have an impact on people, attention will have to be paid to all these factors.

TAKES AWAY BARRIERS

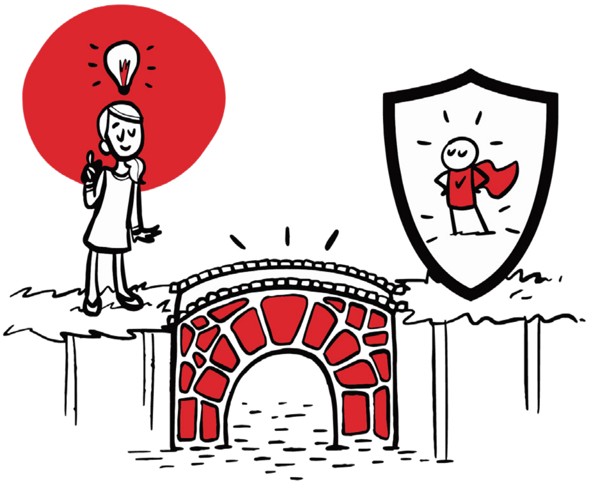
CREATES SAFE BEHAVIOR

Goal

Our vision goes beyond traditional awareness campaigns. After all, practice has shown that the effect of such campaigns is often limited. Awareness campaigns focus on sending knowledge, while people are driven by more than knowledge. In other words; there is a gap between awareness and behavior: knowing what you should do is not the same as actually acting like that!

Awareness is indeed important for effective protection against human error, but not the end goal. That is why Secura developed the SAFE program, which is aimed at bridging the gap between awareness and behavior. **The goal of SAFE is therefore to achieve actual behavioral change.**

In order to actually change behavior, it is important to understand how this works. Therefore, SAFE is a program developed through collaboration between two areas of expertise: that of information security and that of psychology, the science of behavior.



SAFE is based on 5 best practices:

People are not the weakest link, if you....

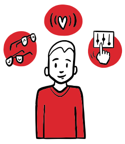
- Focus on safe behavior as end goal
- Combine cybersecurity and psychology
- Focus on all factors of behavior
- Measure what your employees need for safe behavior
- Match the specific needs of your employees by tailored interventions

> "Knowing what to do is not the same as actually acting accordingly!

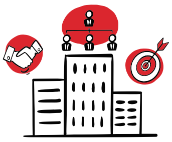
The theory behind behavioral change

Psychology teaches us that behavior is determined by:

Ability - Ability refers to what a person knows and understands about security and about the risks. This is the factor that is most focused on in current approaches such as e-learnings, new rules creation and classroom trainings.



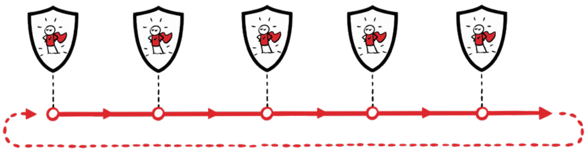
Motivation - In addition to knowledge, behavior is determined by motivation: is someone willing to perform the behavior? Motivation is the result of various personal factors such as experience (has someone tried it before and how did it go?), attitudes (is someone prepared to do some extra effort in return for more safety), perception, norms and values.



Opportunity - The third factor that determines behavior is opportunity: are people enabled to perform the desired behavior? Opportunity is determined by organizational factors. Context and culture are the most important here. The culture of an organization has a major impact on the behavior of employees.

BEHAVIOR = ABILITY × MOTIVATION × OPPORTUNITY

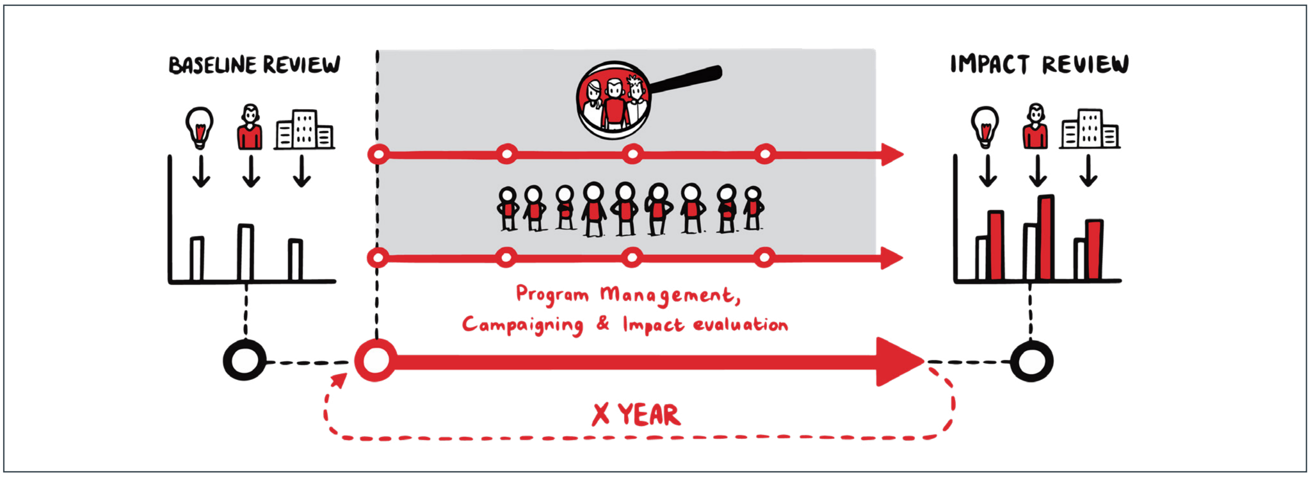
SAFE focuses on **repeated attention for all three of these factors** and thus goes beyond traditional awareness programs that stop at sending knowledge.



In addition, SAFE focuses on carefully identifying the barriers to the desired behavior: why are employees not doing what we would like them to do? Only when it is clear what holds people back from certain behavior, the right steps can be undertaken to remove this barrier. Sometimes this turns out to be a gap in knowledge, but often it is, for example, a matter of lack of motivation, bad experiences or an organizational culture that does not support the goals.

SAFE does not reason from solutions, but from the **cause of the problem**. The solutions that are used from the SAFE toolkit are therefore also different for each organization.

What does SAFE look like?



Baseline measurement

Measurements enable testing the **effect of the interventions**, but also to **define the goals of the program**. The SAFE baseline measurement thus includes a measurement of current behavior, ability, motivation and opportunity. This baseline measurement consists of a variety of methodologies, so it **goes much further than a standard survey**. The outcome of the baseline measurement provides a clear insight into the current status and into which of the factors require extra attention. How does this look in practice?

The program starts with a baseline measurement to enable testing the effect on the interventions. The baseline measurement is aimed at all employees in the organization and consists of:

- **Phishing Emails** (to test motivation of employees)
- **E-learning** (to test knowledge of employees)
- **Roadshow** (to address motivation and opportunity of employees)

Basic program for the entire organization

SAFE consists of a **basic program for the entire organization in which all three factors of behavior receive repeated attention**: Keeping the necessary knowledge up to date, boosting motivation and establishing the right culture. This is done in various ways such as social engineering and road shows. The repeated attention to these three factors is necessary to activate the topic of information security and to remind and enable employees behave safely.

For the whole organization, Secura starts to communicate together with the internal communication department about the various goals of the security awareness program for your organization. Included in the communication is the start of the basic program for the whole organization with e-learning modules. The program offers 26 elearning courses about various topics, such as an introduction into cybersecurity for employees, phishing, malware and privacy related topics. For specialists within your organization we offer GDPR training, OT Security Awareness Training and courses for higher management.

Factor	Intervention to address the entire organization
Behavior	(Addressed by the factors before)
Capacity	E-learning (26 E-learning courses available)
Motivation	Multiple types of Social engineering (Phishing/ Smishing & Vhishing)
Opportunity	Roadshow

Tailored program for focusgroups

In addition to the basic program, a **tailored program runs every quarter for the focusgroup** of that specific quarter. This approach will be repeated in the second year, meaning that each focusgroup will receive repeated attention. For each focusgroup, specific goals will be identified, given the nature of their work: what safe behavior should this group display in each case? Subsequently, a **barrier assessment** takes place to investigate what is withholding this focusgroup from the target behavior.

Finally, these insights are translated into **concrete interventions:** what does this focusgroup need to actually display the desired behavior? This methodology ensures that the actions taken match the needs of the focusgroup. For example, sometimes the analysis will show that the focusgroup benefits most from experiencing the urgency of an incident simulation. Another time it will be about creating support by setting up an ambassador network, or increasing motivation through a hack demo, or a highly targeted e-learning module to update a specific gap in knowledge.

One of the distinguishing features of the SAFE program, is that it does not jump to solutions. In other words; instead of assuming what would help the employees most to behave securely, we put considerable effort into understanding them. What drives them to behave like they behave? So, instead of reasoning from your own point of view, it starts with identifying the barriers and then working to remove them. This will be done by means of some (4 to 5) personal interviews, one on one with a representative sample of employees. The result of this step will provide insight in what is currently withholding people from acting in line with the goals?

Effect measurement

To measure the **success of the interventions** we repeat the methods of the baseline measurement once more in the effect measurement phase:

- **Phishing Emails** (to test motivation of employees)
- **E-learning** (to test knowledge of employees)
- **Roadshow** (to address motivation and opportunity of employees)

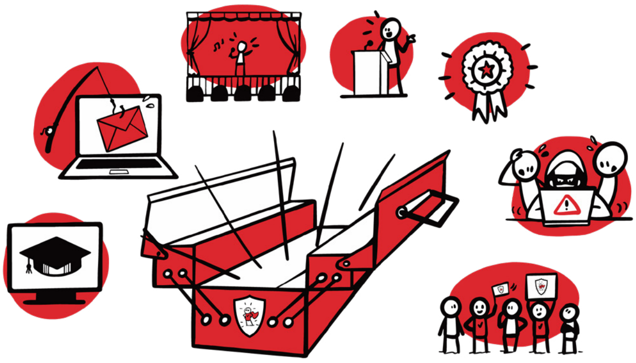
The SAFE toolkit

SAFE has a **toolkit of a carefully selected collection of interventions**. These interventions vary according to their topic (e.g., following strong passwords or rules for document classification), with regard to influencing strategy (e.g., increasing motivation, educating or encouraging), and with regard to resources (e.g., demos, attention grabbers such as posters or video material, or ambassadorship).

Since we do not believe in "one size fits all" solutions, we do not currently know which intervention will be used to achieve the goals for specific focus groups. Most important however, is that the selection of the intervention is **fully tailored** based on the results of the careful analysis that defines the SAFE approach.

In short, the SAFE program differs from traditional awareness programs because it is:

- **designed by psychologists and information security specialists**
- **focused on safe behavior as end goal** (so it goes beyond awareness)
- **focused on all aspects of behavior:** in addition to ability (knowledge), also motivation and opportunity
- **tailored to the nature and risks of an organization** (so no 'one size fits all')
- **developed on the basis of psychological techniques** for behavioral change such as stimulation and facilitation (so it goes beyond training)
- **based on repetition** (so no "one-time check-in-box activity")



Why SAFE?

With SAFE you invest in **creating awareness and achieving behavioral change** that is tailored to the needs of the employees in your organization. As a result, the maturity level of information security increases, making the **organization more resilient against outside attacks**. By choosing the SAFE program, it is also measurably clear, both internally and externally, that privacy and information security are of great importance to you.

be SAFE

SAFE demonstrably makes your **employees more aware and competent** to behave appropriately in case there are attempts by malicious parties to gain access to systems and information. With SAFE, your employees reduce the chance of incidents with a major impact and thus the associated high costs and the risk of reputation damage. **In short: Better SAFE than sorry!**

Interested?

Contact us today:

Follow us:

☎ +31 88 888 31 00

✉ safe@secura.com

safe.secura.com

Shaping a World of Trust