Effective Security Awareness: Learning Approach

More than 80% of all cyber incidents are caused by human errors. Enterprises lose millions recovering from staff-related incidents – but the effectiveness of traditional training programs intended to prevent these problems is limited and they usually fail to achieve the desired behavior and motivation.

Inadvertent employees' errors are responsible for the most of cybersecurity incidents in organizations today:

- IBM reported in 2015, that the percentage of the internal **breaches caused by human errors exceeds 95%**[i];
- **75% of the U.K. large organizations** and 31% of small businesses **suffered staff related security breaches** in 2015[ii];
- **Average financial impact** of an incident involving careless actions of employees is **$865,000 per breach**[iii];
- **Average cost of phishing attacks is up to $400 per employee per year** (other types of cyberthreats are excluded from this count)[iv];
- Insurance from incidents caused by human errors, mistakes and negligence are reported to be **covered by only 25% of the cyber insurance plans** (while risks caused by external cyber criminals are covered by 84% of insurance plans, and risks from malicious or criminal insiders are reported to be covered in 75% of cases)[v].

Analysis has shown that the majority of existing Cyber Security Awareness training programs are ineffective:

- Reading policy documents and instructions is boring, too technical, too skeptical, i.e. full of treats and "Don't", without showing examples of safe behavior;
- People are not motivated to learn (only 22% believe they can be targeted by criminals);
- Employees do not see IT Security as partners and always try to bypass them;
- There is a lack of measurements on awareness, besides "how many people got trained.

Kaspersky Lab has launched a family of computer-based training products that utilize modern learning techniques and address all levels of the organizational structure. Our training program has already proved its effectiveness

Factors of Learning Efficiency

Understanding of what lies behind any learning and teaching process helps identify reasons of many awareness programs failure as well as define how to build effective educational programs.

First, people learn only when they are motivated. Kaspersky Lab investigations show that people have a set of core misconceptions, which prevent them from cyber safe behavior and demotivate from learning. We look at each of these misconceptions, understand how to change people's perception of them, and create ways to overcome unsafe behavior on a long-term basis.

Second, most awareness programs provide employees with knowledge while it is not what really drives people's behavior. Behavior is the actual target of awareness, and it cannot be formed by solely giving a set of rules or telling people a number of "don't". The goal is to create skills, give positive role models and habits, and reinforce. That is what forms behavior – and the behavior is exactly what is needed from employees in terms of cybersecurity.

Third, people tend to follow the flock. They repeat the patterns of behavior prevalent in their community/company. People do what they believe in, but they are heavily influenced by others. Thus, the key goal of any educational program is to shift a focus from 'pure' technical skills to *motivation*.

The integral approach which Kaspersky Lab uses to fight all of these obstacles lies in a field of modern learning techniques, combining gamification, learning-by-doing, group dynamics and reinforcement. Of which gamification is a key, accounting for both reframing of peoples' attitudes and building new behavioral patterns, not to mention its ability to create strong emotional ties and thus contribute to motivation to learn.

Training Outcome

up to	not less than	up to	more than	strong
90%	50%	93%	30x	86%
A decrease in a total number of incidents	A decrease in a monetary volume of incidents	Probability of using the knowledge in the daily work	ROI from spending to the security awareness products	Willingness to recommend the program

[i] IBM 2015 Cyber Security Intelligence Index.
[ii] 2015 Information Security Breaches Survey. HM Government in association with InfoSecurity Europe and PwC.
[iii] "Business Perception of IT Security: In The Face of an Inevitable Compromise", Kaspersky Lab, 2016.
[iv] Calculations based on Ponemon Institute, «Cost of Phishing and Value of Employee Training», August 2015.
[v] 2015 Global Cyber Impact Report. Ponemon Institute LLC.