10 PRINCIPLES OF EFFECTIVE SECURITY AWARENESS

DISCOVER THE KEY PRINCIPLES
AND RAISE THE LEVEL
OF CYBER SECURITY

SecurityInside

LOGICALTRUST

00

INTRODUCTION

Cybercriminals mercilessly exploit unconscious employees, steal information and paralyze operations of companies. They demand a ransom for data recovery, threatening to publish valuable documents online.

Effective and systematic education, training and awareness-raising can help reduce the financial losses associated with security incidents.

GOAL

After 16 years of performing security tests and educating employees, I know that preparing an effective Security Awareness program is not an easy task.

I hope that this mini guidebook will help to raise the level of security culture in your organization.

Borys Łącki
Security Ninja
LogicalTrust.net

01

SECURITY = BOREDOM

> *Employees have safety in (...) security policy.*

Employees of security departments are often passionate persons and think that everyone should be interested in *cybersecurity* at least as much as they. Unfortunately, such thinking makes them less likely to reach their colleagues.

Watch out for your *ego* - it is often our job to show other people's shortcomings in education, in the field of safety.

Keep in mind that our role is to help, not just to point out mistakes. The latter reduces the motivation of employees to engage in the security.

An employee is not interested in the security, it is not his/her primary duty. Just because it is very important to us does not mean that it is the same for our colleagues.

02

SELECT THE ESSENCE

Perform threat modelling for your company.
Think about what is the greatest danger and educate only about the most important aspects.

Security covers over a hundred different areas, including: physical security, cloud, employee awareness, phishing, etc.
Employees of security department would like to teach their colleagues everything about security, it's a mistake.

Don't overwhelm your colleagues with thousands of issues. Focus on crucial and current threats.

With the limited attention of employees, is it worth talking about possible attacks by fax today? Maybe it's better to focus on malicious attachments, which we often deal with today.

Remember to assess which risks in the company are the greatest and start education from them.

03

MAKE THE BRAIN HAPPY

Dry facts don't work. It's the stories that are the best way of effective communication - this is how the brain works.

If you build a narrative in education on technical details, the brain quickly stops acquiring information.

WRONG: As a result of the lack of update to the CVE-2020-0901 vulnerability, the malware took advantage of the buffer overflow error, allowing it to escalate to user level with the highest privileges and resulted in a loss of availability in the key area of server resources.

CORRECT: I met a colleague the day before yesterday from a company that has an office two floors above us. One of the employees clicked on the attachment with the virus and cybercriminals took over their computers. The IT department is still trying to recover the stolen data, they have already lost several hundred thousand EUR and were forced to fire three people.

04

ADJUST THE MESSAGE

Organizations and people are different. Remember that.

Use the methods suitable for your company and your co-workers.

Apply the top-down principle.

Tell different stories to administrators, different to office workers.

Remember, fear is demotivating. Don't point out mistakes to specific people, it's better to show that there is a general problem in the organization.

Try to play to one goal and together with your colleagues, build an effective human firewall.

05

WHY?

Remember to explain why sth needs to be done.

WRONG: The rules relating to the password security need to be followed.
The security policy states that a password should consist of a minimum of 12 characters, 2 capital letters, 4 special characters and 1 number.

CORRECT: Explain to the employee why he/she should use complicated passwords. For example, tell them that if they do not use strong passwords, cybercriminals can steal data from the company, the company will lose money and can be forced to reduce premiums.

Research shows that while understanding why we should do something, we act more effectively.

06

RESPECT EMPLOYEE'S TIME

Nowadays education means a struggle for human attention. If you want an employee to spend an hour a week on security issues (which are not his/her interest), the effectiveness of education will be very low.

Quality is more important than quantity. On our e-learning platform, each lesson lasts several minutes and contains a film that is enjoyable to watch. Only a short and interesting form will make education not be perceived as something unpleasant.

Remember to lower your friends' pain threshold, so they will be more willing to come back to the security issues.

07

PERSONAL PROFIT

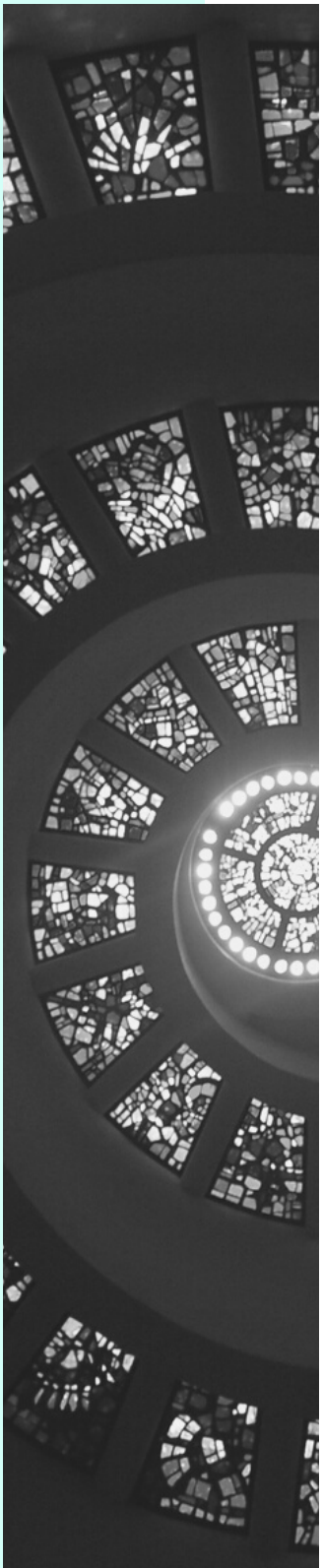
"You have to do this because it's important." - doesn't work. It is more effective to emphasize the personal benefit.

The fear that the company will lose important data is not convincing for the employee. **It is worth adding a personal context to education**. An employee may lose his or her private data, e.g. photos from holidays or money from a bank account. In this way, we will teach the employee good practices, which he/she will transfer to the company.

The personal benefit can be broadly understood. It can be the protection of sensitive data and money, but for some people there can be more valuable things e.g. a game character created for years :) It is important to reach people's hearts and understand their needs.

08

ACT IN A PROCESS AND SYSTEMATICALLY



Plan your activities for at least a year ahead.

Analyze your budget, think how to spend it optimally. Consider what you can do with your internal resources, where it is worth to use free materials, and in which activities you need to get support from an external company.

Act systematically but not too often. A one hundredth email warning about dangerous messages will be ineffective. **Act less often but more interestingly.**

It is worth sending out the newsletter on the same day of the week at the same time, however, you should do the socio-technical tests at different times.

At least once a year, provide a lecture in an accessible form and perform social and technical tests. The "wow" effect will stay in the minds of the employees for several weeks.

The employee should have access to the e-learning platform all year round to use it flexibly.

09

SIMPLY AND PRACTICALLY

The advices should be understandable and useful.

Only solutions that are easy to remember and convenient to use are able to make employees use them.

If you want the employee to use different and complicated passwords, then tell him/her how he/she can easily remember complicated passwords and teach him/her to use the password manager.

10

CATCHY FORM

> *One picture is worth more than a thousand words.*

Remember that the attractive form can catch the employee's attention for a few minutes. The world is crazy about short films, why not use them in raising awareness? An interesting static or moving image is more effective than written content.

Take care of content diversity and invest in various strategies for reaching out to the employees.

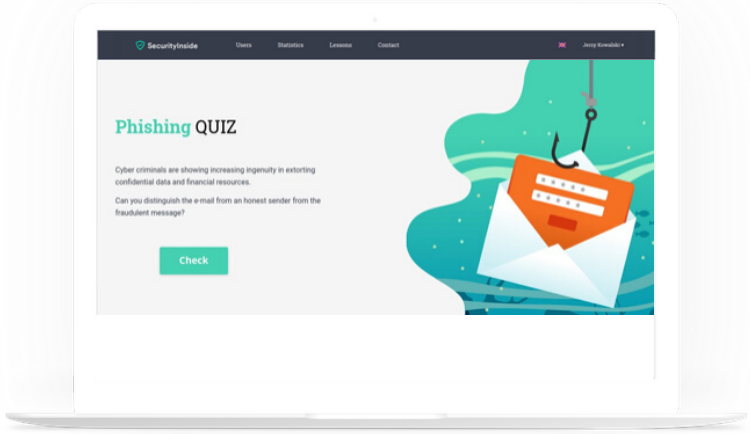
Printed posters, newsletters sent by e-mails, graphics, films, e-learning, interesting gadgets, social engineering tests, live lectures. Every well-chosen communication channel increases the effectiveness of education.

Think unconventionally. Maybe instead of dozens of standard e-mails with the phone number to the security department (which nobody reads), it's worth printing interesting graphics and put it in the right place.

CONCLUSIONS

1. Security is not the most important thing.
2. Educate on key issues.
3. Use stories, not dry facts.
4. Match the form and content of the message.
5. Explain why?
6. Quality, not quantity, less is better.
7. Emphasize the personal benefit.
8. Act in a process and systematically.
9. Advice should be simple and useful.
10. Take care of a diverse and attractive form.

FREE MATERIALS



https://quiz.securityinside.com/

Can you distinguish the e-mail from an honest sender from the fraudulent message?

FREE MATERIALS

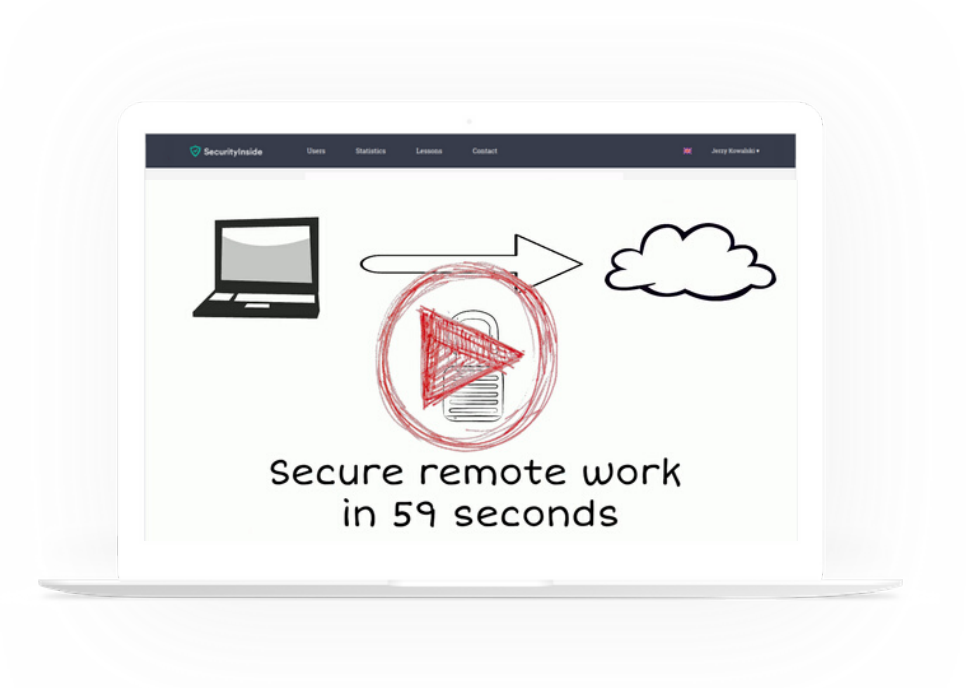
Posters - the "rebel" campaign

https://securityinside.com/free/files/securityinside.com-infographics-201903-pl-jpg.zip - PL

https://securityinside.com/free/files/securityinside.com-infographics-201903-en-jpg.zip - EN

FREE MATERIALS

Video - safe remote working in 59 seconds



https://securityinside.com/free/video/bezpieczna_praca_zdalna_w_59_sekund/ - PL

https://securityinside.com/free/video/remote_secure_work_in_59_seconds/ - EN

SecurityInside

LOGICALTRUST

OUR SERVICES

- PENETRATION TESTS
- E-LEARNING
- CONTENT, REPORTS, POSTERS
- LIVE AND DIGITAL TRAININGS
- SOCIAL ENGINEERING TESTS

THEY TRUST US

orange, pepsi, STATOIL, Multikino, GlaxoSmithKline, Hewlett Packard Enterprise, Santander Consumer Bank, Alior Bank, RBS, AEGON, Crédit Agricole, Getin Noble, Viessmann, money.pl, Energa, PKP Informatyka, Ministerstwo Finansów, PWPW

YOU ARE WELCOME TO CONTACT US

OFFICE@SECURITYINSIDE.COM
HTTPS://SECURITYINSIDE.COM
+48 71 738 24 35