How To Spread Password Positivity

MATESO
PASSWORD SAFE

How to Guide

When Your Security Concept Misses the Employee

Your security concept is set up and ready to use? The white paper is spread via mail and all your employees "should now know" how to handle their passwords and security overall? Are you sure? Do you know for certain that all your companies passwords are safe and sound? You probably can't tell. In fact, according to Bitkom, one in three online users uses the same password for multiple services. These are bad habits that just don't get away easily. So how can your company develop more security awareness?

What Doesn't Work

Did you know that cyberattacks and the like are not as shocking to your employees as you might expect? Sure, at first news about security incidents may still be shocking. But attacks are becoming more and more frequent and news about cracked passwords are now almost part of everyday life for us. As people become accustomed to such incidents, it becomes more and more difficult to deter them and is hardly sufficient to ensure a long-term improvement in security behavior. Nevertheless, employees are told not to do this or that, and supervisors try to persuade them to implement them with possible consequences or to build up threatening backdrops.

"If you click on links like this, you will open the door for hackers to come into our network and steal everything."

Scary enough for a short-term effect? Better think ahead!

Fear As Blocker

Why do they do this? Because fear is a powerful emotion! However, by scaring employees, you can even achieve the opposite effect by making them even more insecure on how to act in new and potentially danger situations. This fear then hinders them on thinking clearly and ahead. Or your employees might think that the scenarios are exaggerated scare tactics and do not take them seriously in the first hand.

Yes, fear is a powerful emotion. But it is also just a short-term feeling. It can bring your employees to change their password once or to think up one very complex password. According to a study by IGS, over 85% of respondents believe that pressure is used as a management tool. According to the study, the consequences of this are less willingness to perform, commitment and loyalty. In the long term, therefore, fear and pressure can have a rather deadening effect on employees.But when fear has passed, the old habits will creep back in: A special character is simply added the next time the password is changed, and so on. And the remaining fear will still resonate as a silent warning, preventing your employees from working productively.

When employees fear to make mistakes, the risk is even higher that there will be errors, because fear leads into insecure behavior. So they will, for example, mistype their password during login more often or no longer find the safe place for their password that they picked out in a hurry after the last warning.

This is because fear causes employees to act on impulses rather than logically and information-based. Simply adding a number to a password can be done on impulse, as can be quickly hiding the password on a post-it under the keyboard. **So even though, fear is a powerful feeling, it can become counterproductive for your company when used as means to an end.**

Following Rules That Are Out of Reach

A question, companies should ask themselves: “Does my employee already have everything he needs to stick to the rules that have been set up internally?” When it comes to passwords, it can be demanding and sometimes even impossible for employees to stick to these rules when they don‘t have help or the right tools for it as well. For example, employees are told to only use unique passwords for every account, change it every 3 months and to not write them down. It is often overlooked that with an average of 26 passwords per employee, a lot of effort and hassle is involved.

So what happens is, that the employee will give up or find workarounds like shadow IT. The problem therefore only appears to have been solved, but along the way, people and their needs were ignored. From this example, it becomes increasingly clear how important it is to introduce a Modern Workplace, which also forms IT security as the cornerstone of compliance and also provides tools and processes for implementation.

Focus on people

Modern Workplace as an interplay of devices, technologies and software

- Whether in the home office or on the road: enable different working environments
- work-life balance? Considering working conditions
- From open door to standup desk: Creating a feel-good atmosphere
- Security enablement: offering tools and services

What Really Works

Why We Do This: Create Understanding

When it comes to rules, we often present them to the audience and say: “This is what we will stick to now as the government / the management / other policies tell us to do so.” So we spent a lot of time in telling our employees that this or that is important. We remind them regularly to stick to these guidelines and check their behavior from time to time. But what is missing, is a true understanding on the other side. And this is not about frightening them with potential consequences for them or the company. It is about creating security awareness little by little and focus on the positive outcome when the rules are adapted. “if we only add two special characters to a password, hackers would already need x more time to crack it.” or “If we change our passwords regularly, we can increase our internal password security by x %.” This way you don‘t make your employees feel like they are part of the cause of a problem that needs to be eradicated. **They are part of a positive change and an active and important part of the solution they are contributing to with their commitment every day.**

Find the Right Arguments for Your Employees

To live a positive password culture in companies, the right arguments count for employees. As hard as it may sound – your employees care less about password security than you do. Because productivity to them – and to log in easily belongs to that – is more important than security for them. They have deadlines they have to meet, calls they have to take and projects they have to finish. Login and co. are perceived only as a necessary evil.

So how do you get your employees on the safe side? By making their work easier and showing them added value for themselves: If your employees see security as something positive that will actually help them in their daily business, they will see the use of ist and be happy to participate in it in a long run. This is why security should be seen as enabler and not as a stopper.

More productivity with Password Safe
What the tool does for your employees – No more ...

... thinking up and remembering passwords: Secure passwords (in accordance with internal password guidelines) are created at the click of a button.

... searching for passwords: All login data is stored securely and clearly in Password Safe.

... failed logins or mistyping of passwords: The right login data is transferred automatically.

... having to give passwords to colleagues on paper: Passwords are already automatically made available to the appropriate users or can be assigned easily.

... manually resetting and replacing passwords: With automatic password resets in Password Safe and the application itself.

How We Do It

Provide Training

Instead of punishing employees when they made a mistake, they can be trained towards a positive password culture that lasts in the long term. This includes creating a pleasant working atmosphere for employees, appealing to their team spirit and encouraging them to see themselves as an important part of the company. Only in this way will it be easier for them to confide in and cooperate in the event of a self-inflicted error, without immediately sweeping it under the rug out of fear of possible consequences.

So does it even make sense to gather all employees in one room per quarter and talk about safety issues for a few hours? It won`t hurt, but it's not enough. The real training takes place in front of his desktop in everyday working life for the employee. This is when the knowledge is being applied practically in those moments. And often when there is no one available to provide support or to keep an eye on safety behavior. **So training does not mean a specific date where employees have to show up.** Training takes place every day and every time the employee comes into contact with safety-critical processes. So how can you solve that?

Ask yourself:

"Do your employees see trainings only as mandatory event or do they participate willingly and perhaps even voluntarily out of their own interest?"

Address Problems Correctly

Is it really the fault of your social media manager that he didn't change all of his passwords after 2 months or should that maybe have been the task of IT? Is this demand even something your employees can do or should a tool do it for them? Is it really their fault something doesn't work or is it maybe the fault of management who looked away way too long? These are sometimes hurtful questions for a company which only make them even more important. As multiple organizations like the National Institute of Standards and Technology (NIST) have already recognized and correctly assigned the problem, they highly recommend password managers to support employees with the password problem and not to leave them alone with their needs.

As easy as it may sound:

You want your employees to work? Give them a workstation. You want your employees to only use strong passwords? Give them a password manager.

Power Users As Bridge Between Technique and Humans

You need security staff with an open door philosophy and mindset. So this security personell must not only understand IT, but also the human in front of them to built a trustworthy relationship and to be able to respond to them properly. Only then, employees will come talk, communicate transparently and cooperate so that you can find the best possible solution.

To achieve this, employees outside of IT – like one from sales, one from finance and one from marketing – can be selected as security promoters. They should be trained as power users of the relevant tools like Password Safe to be able to help their colleagues properly. These security promoters do not only receive special training, but they also communicate closely with their teams to spread password positivity within and be a role model when it comes to the right password hygiene. This power user is there to support his colleagues day to day, is always there if a question pops up and offers help when needed.

What power users need:

- leadership, explanation and communication skills
- technical affinity
- be well networked and have a good standing in the team
- be able to inspire someone even for complex topics

For example, an employee may come to him on how to share a password securely with a colleague or on how to use access data together with an external agency. The power user not only shows him how to do this in Password Safe, but also lets him practice by himself while still being available. So the mere presence alone can eliminate the fear of contact with new tools and processes and makes employees more confident in using it, thus reducing the frequency of errors.

Training Is Not a One-Way Street

In return of learning from power users, these can also gain essential insights about the hurdles, problems and needs of employees that IT themself maybe hasn‘t even been aware of. So it is a win-win situation for the whole company and tools and processes can be aligned even better. And that‘s not all: With a dedicated person to go to in your team instead of one training for every employee once in a while, the employees will more get the feeling that a positive password culture is a team effort everyone contributes to directly.

“Can I bother my security promoter right now with this? Maybe it‘s written somewhere and I missed it or should have known that by now ... Should I write an email, choose chat or would it be ok to call quickly?”

Do You Have the Right Communication Channels?

When it is not really clear how to address somebody in which way, employees become insecure and choose to keep their problem to themselves and try to “solve” it on their own. This unsafe behavior can pose great danger to companies.

Especially in times of working from everywhere, it is important to have direct communication channels so employees can reach out easily when they need guidance and assistance.

Security promoters can, for example, set up a dedicated channel for password problems in the team, where people can post 24/7, and hold short dailies that anyone can attend if they have an acute problem. No matter how your team will implement direct communication channels: The important thing is that it is communicated clearly and transparently to them.

Believe In Your Employees (and Show It)

What is the opposite of fear? It is trust – trust in one`s abilities, trusting that the employee will make it work and you believe in them. But how can you show them that when it comes to such a dangerous topic which could cause a security incidence? By giving them more room to explore the topic securely and support them in this.

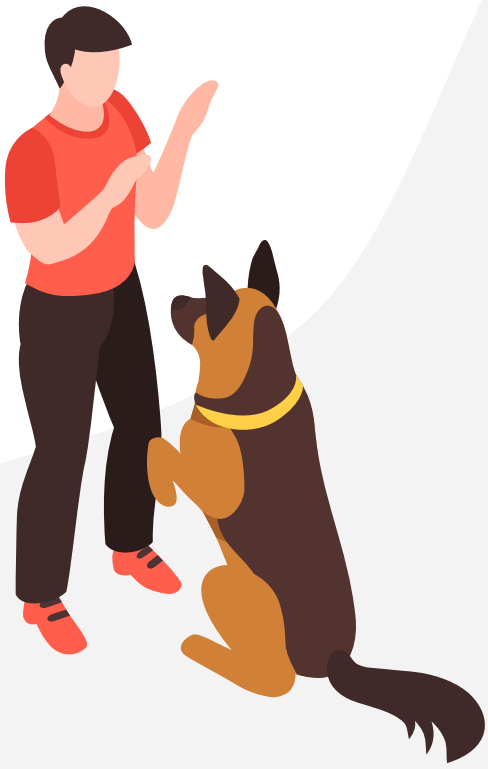
To let them explore, you can at first implement password policies theoretically. With the option to check passwords according to the implemented policies in Password Safe, the user can at first by himself try and find out if he understood what a secure password should consist of.

And then you can even reward password-positive behavior. For example, the employee with the strongest password quality in the last months becomes “Password Pro” in your company – maybe with the possibility to become a power user. This is how you create positive experiences and motivate employees to repeat them. This will make them more confident in themselves and their abilities so they will be less likely to make mistakes and spread password positivity in the whole company!

Password Management The Pavlovian Way

To some people the pavlovian dog may say something: It originates from the well-known empirical experiment of the Russian researcher Ivan Petrovitch Pavlov, who thus provided proof of classical conditioning. According to classical conditioning, a new, conditional reaction can be added to a natural, usually innate, so-called unconditional reaction by learning. With Pavlov‘s dog this meant that he got food when a bell sounded. After several runs, the dog responded to the bell sound by increased salivation alone.

Based on this, security expert Lance James proposed Pavlovian password management. This is intended to train users in the long term to select passwords that are as secure as possible. When using a weak password like “test123@#” that could be hacked after 4,5 days, the user would be invited to change it after 3 days already. With a more complex password, the user would have 3 weeks time and using a paraphrase he would even be rewarded with a time span of 90 days. With this method, users should be conditioned to use increasingly complex passwords. This method can be adapted for different reward mechanisms.



Human Error or Just Human?

As a negative password culture only relates to what NOT to do, it only focuses on bans and possible consequences more than chances and causal research. Compared with this, a positive password culture always offers a solution to the original problem: So the employee is not just seen as “human error” which has to be avoided and left out as well as possible. It is seen as a “human being” with its needs, strengths and weaknesses in focus.

So the company can develop a security plan that involves them best and thus closes security gaps as long as possible. This means pushing the confidence of every employee of yours and making security not hard to understand, but easy and even fun to implement individually. And not enough: A positive security culture that focuses on communication as well increases the chance of employees telling the IT when something already went or might go wrong in the future. So the potential damage can also be kept as small as possible.

Stop thinking of “Human error”, “DAU” or “Layer8”

Make employees not part of the problem, but part of your solutions!

Excursion: Where Password Positivity Thrives Best

Working from home has become the new normal as Corona forced us to do so very quickly in 2020. Are employees happy with this? Apparently and according to studies they are. Some companies were initially afraid about sinking productivity when working from home. But they where mostly wrong as employees wanted to do justice to their new-found freedom to work at home and did not want to gamble with it under any circumstances. In addition, they could now work (better) in a more undisturbed and relaxed manner with fewer distractions. Which also means less visibility for the employer as they are working in their one home network or maybe even from an open network in a coffee shop nearby ...

So do you need your employees in the office to generate more security awareness? Certainly not: The trust placed in employees working from home reinforces the belief that their previous password behavior is valued and rewarded. And a trusting relationship in which cybersecurity is experienced as positive and motivating – combined with the right tools and security precautions like VPN and a password manager – can work from anywhere!

Summary: Remember To Stay Positive

Negative Password Culture	Positive Password Culture
• targets only short term goals	• targets long term goals
• extrinsic motivation: no influence on higher priorisation of security	• intrinsic motivation: employees “live” and internalize the methods
• security = stopper: employees avoid / ignore security standards out of incomprehension	• security = enabler: employees see their own positive benefit for their work
• making security harder as fear blocks thinking	• making security easier applicable and usable for everyone
• works through one-sided training, too little exchange and punishment mechanisms as well as threats	• makes security personnel available to solve problems, educates employees, and rewards security-centric decisions
• hinders productivity as rational choices are blocked	• increases productivity, as own use is recognized and applied
• negative atmosphere provokes proximity of more (avoidable) mistakes	• pays off on positive working atmosphere which also ensures fewer errors

Tips At The End: How To Spread Password Positivity

- **Exemplify safety:** Your employees need role models that guide them their way. For example, you can integrate Password Safe power users / evangelists that function as direct contact person in the company if questions pop up or employees nee guidance.
- **Put theory into practice:** Do your employees have the right tools to put safety pre cautions into practice? Make sure the way of using them as easy as possible and offer introductions, tutorials and help in using new tools.
- **Create a positive experience:** Forgotten their password? Don‘t know how to share it with team members? Make sure that you really listen to your employees needs, take them seriously and offer them secure solutions to solve their problems.
- **Reward password-mindful behavior:** Praise team members who address security issues, need help or share their password experience so they will be more likely to share issues in the future.

Author:
Kristina Kaya
Product Marketing Manager

MATESO
PASSWORD SAFE

MATESO is a leading German IT company, which has successfully established in the DACH region since the company was founded in 2006. The developed password security solution Password Safe is distributed internationally by its worldwide partner network. Well-known references testify to the technological and know-how advantage of the IT software.

Today the constantly growing enterprise registers over 10,000 corporate customers with several million users worldwide - including 21 Dax 40 companies.

Pioneer in Enterprise Password Management

Password Safe serves companies as a central digital safe for securing, managing and monitoring sensitive data such as passwords, documents and secrets.

MATESO GmbH
Daimlerstraße 15, D-86356 Neusäß
Web: www.passwordsafe.com
E-mail: sales@passwordsafe.de
Tel: +49 821 74 77 87-0

MATESO
PASSWORD SAFE