

## Protect your company from phishing attacks

### Main functionalities Koala Corporate



Full access to okKoala system for managing phishing campaigns



Unlimited number of messages sent and campaigns created



Detection of users posing the greatest threat



Advanced reports and transparent presentation of data



Database of dozens of ready-made phishing message templates with a wide range of topics



Possibility to create and add your own email templates



Tagging employees and grouping them into thematic groups, e.g. according to the company department



Convenient and fast data import



Training and examinations to increase staff knowledge and alertness to cyber attacks



Safety certificates for employees who achieve the best results in training and examinations



Clear and convenient documentation to make the service easier to navigate



Microsoft account login (SSO) and double authentication (MFA)



Possibility to add multiple administrators with different permissions



Trainings with gamification and prizes



Full automation of the training and campaign process



Export of report data and possibility for additional analysis



Access to a campaign imitating computer encryption and bitcoin ransom demand



Access to an immediate campaign to attack employees



Access to a monthly training campaign detecting the weakest link



Access to a campaign imitating theft of MFA to Microsoft Office

## Protect your company from phishing attacks

### Extended description of functionality

#### Koala Corporate



##### **Full access to okKoala system**

Full access to all functionalities of the okKoala system in the corporate version and all the latest updates and novelties that will appear during the contract period.



##### **Unlimited number of messages sent**

Throughout the whole period of the cooperation you can send unlimited number of e-mails to your employees and conduct any number of campaigns and trainings! We enable you to make every effort to educate your employees and increase data security.

\*Each employee may be involved in only one campaign at a time, e.g. if an employee is included in a campaign lasting a week, he may be added to the next campaign / training only after finishing the previous one, i.e. after a week.



##### **Search for major threats**

Identification of employees who pose the greatest threat to data security in the company. The service detects the most vulnerable people, identifies them in the report and trains them to increase security.



##### **Advanced reporting**

Get detailed information about the campaign. You will find out: who opened a message that may have contributed to data loss in your company and when; who failed to report that an "attack" occurred; how many people clicked on malicious links and read the message; how data security levels are developing; who entered the training, what the outcome was, and who ignored it; who has the greatest resilience in your organization; what department is most vulnerable; and other useful information.



##### **Base of ready-made templates**

We have prepared for you a set of the most popular Phishing Attacks, which took place in Poland, Europe and the world. This database is constantly updated by us and you can use it without additional charges. We prepare templates in Polish and English in such a way as to convince as many users as possible to click. Almost each of our templates is signed by name to the sender!



##### **Create your own templates**

To increase the effectiveness and credibility of "attacks" you can create your own templates, which correspond to the communication standards in your company. Add your own templates and send them from your own domain and make sure you catch your employees!

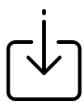


##### **Tagging of employees**

Bring your employees together in teams, departments or risk groups and create a separate dedicated campaign for each of this group. This will increase personalisation and effectiveness.

## Protect your company from phishing attacks

### Extended description of functionality Koala Corporate



#### Data import

Adding multiple employees can be tiring, so you can easily import their data and tags from a csv file. Of course you can as well add them manually.



#### Training and examinations

Specially designed training courses to increase your employees' awareness of phishing and teach them how to recognize dangerous messages. The trainings are gameable and last an average of 30 minutes, so it does not disturb the daily work in your company.



#### Certificates

Trainees will obtain personal safety certificates after reaching a minimum of 80% of points, which are valid for one year.



#### Technical documentation

Extensive documentation will make it easier for you to use the okKoala portal efficiently.



#### Protect your account

Keep caring about your safety! Secure your account using double authentication or log in with your Microsoft account.



#### Many administrators

If several people in your organization need to have access to okKoala, simply add them to the system and set the level of access to functionality.



#### Gamification

The gamification of training helps to absorb the maximum attention of the employee and provide them key information in a short time. Additionally, your employees can compete with each other and win prizes!



#### Process automation

The message dispatch process is fully automated. Once the campaign has been set up in a few simple steps and started, everything will be carried out by our system and you will be able to enjoy detailed reports.



#### Export of data

Do you want to create more extensive reports on your own, based on the data you have collected? Export files and create your own report on external systems, such as Microsoft Power BI.

## Protect your company from phishing attacks

### Extended description of the campaign **Koala Corporate**



#### **Monthly campaign**

Recommended campaign to test your company's resistance to phishing attacks. The whole campaign lasts one month. During the first 2 weeks, phishing messages are sent out in a random order and at random intervals to identify people who pose a threat to data security in your company. Those who click on a sent message will immediately be redirected to training to make them aware of the threat of phishing and to learn how to recognize suspicious messages. In the next stage of the campaign, an invitation to training is sent to all participants. Those who have not been caught before are congratulated. This allows everyone to broaden their knowledge and take part in the competition. One week after the training, another phishing message is sent to all participants, which tries to catch inattentive people and allows to verify the effectiveness of the training. Everything is finished with a detailed report in a live version. Additionally, the campaign allows to identify and mark employees who pose the greatest threat to data security. It also suggests recommended actions in relation to each employee.



#### **Immediate campaign**

A campaign to check a specific group of people or the whole company at once. It consists in immediately sending a selected phishing message to selected people and checking their vigilance.



#### **The Bitcoin campaign**

The campaign checks how employees react to a computer attack. When someone clicks on a phishing message, the computer screen simulates the process of disk encryption and data theft. Finally, the user sees a proposal to pay the ransom or bargain. If such a person does not report it to the right person in the organization - concealing the information exposes the organization to losses. Once such people are identified, training can be provided for the risk group.

[Link to presentation](#)












#### **Office Campaign**

The campaign allows you to test the effectiveness of an attack on a multiple authenticated Office 365 account. The user is asked to log in to a copy of the real Microsoft office log-in page to steal account access and access all resources in the cloud. The result of this campaign is a list of people who could, due to lack of awareness of such an attack, break their own company's security, basically helping cybercriminals. Finally, the participants are redirected to a training course, that educates the employee on how to prevent phishing attacks and fake sites.

[Link to presentation](#)

## Protect your company from phishing attacks

### Price list for additional services

	Onboarding - individual training in the use of okKoala system			1 hour - 59€
	A package of dedicated templates made according to the customer's instructions and requirements	3 pcs. - 499€	6 pcs. - 899€	9 pcs. - 1 299€
	Expert advice on creating and planning new campaigns			1 hour - 59€
	Dedicated consultant who conducts campaigns and trains your employees throughout the year, providing you with regular reports on the actions and situation in the company			4 999€
	Consultation with a certified cyber security expert			1 hour - 149€
	Remote training for a group of up to 290 people related to cyber security and safe remote working - scope consulted with the client		2 hour - 999€	1 day - 2 999€
	Solution Assessment Cyber-Security	up to 200 empl. 3 000€	up to 1000 empl. 5 000€	over 1000 empl. Custom
	Management, property, group, life, pension, PPK, health and much more insurance provided by AVIVA			Individual pricing
	Microsoft cloud software licenses and implementation of Microsoft services			Individual pricing

## Protect your company from phishing attacks

### Description of additional services



#### Onboarding

Training in the use of okKoala system, during which our specialist will present all possibilities and functionalities of the service, train people delegated to administer the system and answer all questions. Yes, only 60 minutes is enough to fully operate our platform.



#### A package of dedicated templates

As part of the template package, our graphic designers will make a number of dedicated email templates for you, according to the guidelines and information provided. This gives you the opportunity to personalize your messages according to the company's realities and standards.



#### OkKoala expert advice

Our expert will help you prepare an effective training strategy. He will advise you which configurations will be most suitable for your company and how to achieve your goal in the most effective way.



#### Dedicated consultant

Our dedicated consultant service is prepared for people who are not interested in personal management of the entire platform and only expect information about the safety of their company. It is a person who prepares and carries out phishing and training campaigns for you. We will send you regular reports including activities carried out and informs about the irregularities found.



#### Consultation with a certified Cyber-Security expert

Have you got suspects about your company not being fully security prepared? Has there already been an incident? Do your employees work remotely without proper training and risk to manage mistakes? Our consultant will help you take the right direction and point which areas, need to be secured in your company.



#### Online group training

Group online training conducted by our expert in cyber security and safe remote working.

## Description of additional services



### Solution Assessment Cyber-Security

Solution Assessment is a study to analyze the effectiveness of software used in an enterprise in terms of cyber security and cost optimization. It allows to identify potential threats that may violate information security and prepare a plan for their protection. An additional effect of the study is an implementation project, which contains a list of possible improvements in the company's IT infrastructure, e.g. new software, cloud migration, insurance against cyber attacks.



### Life and non-life insurance

Life insurance dedicated for management boards, group insurance for employees, property insurance with third party liability, reimbursement of medical expenses, hospital stays, treatment abroad and many others. For more information ask us for dedicated offer.



### Microsoft licenses and services

We are an authorized Microsoft partner, we can prepare for you a valuation of Microsoft cloud software licenses (e.g. Microsoft 365) at preferential rates. We also assist in the implementation of IT projects created during the Solution Assessment.