

Darbinieku kļūdas: joprojām lielākais kiberdrošības drauds
(bet ir arī risinājums)

Imants Felsbergs
Biznesa attīstības vadītājs

Datu incidentu seku novēršanas vidējās izmaksas, 2020



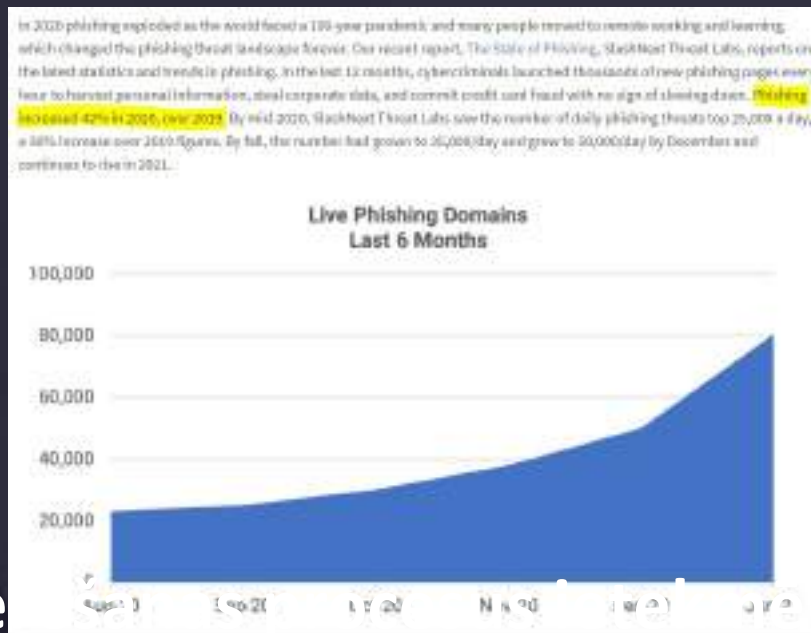
90% datu incidentu pēdas ved
pie gala lietotāju pikšķerēšanas
uzbrukumiem

(Verizon)



Pandēmijas
apstākļos
pikšķerēšana ir
saasinājusies vēl
vairāk!

Kā pikšķe



Deloitte.

Services ▾

Industries ▾

Careers ▾

The case for increased cybersecurity

The increase in remote working calls for a greater focus on cybersecurity, because of the greater exposure to cyber risk. This is apparent, for example, from the fact that 47% of individuals fall for a phishing scam while working at home. Cyber-attackers see the pandemic as an opportunity to step up their criminal activities by exploiting the vulnerability of employees working from home and capitalizing on people's strong interest in coronavirus-related news (e.g. malicious fake coronavirus related websites). Another important consideration is that the average cost of a data breach resulting from remote working can be as much as \$137,000.

On July 8th, the City of London Police reported that since January 2020 more than GBP 11 million have been lost due to COVID-19 scams. In Switzerland, one in seven respondents to a survey had experienced a cyberattack during the pandemic period.

TechRepublic. Search 50 Developer COVID-19 More Newsletters Forums Reso

Its Psychology of Human Error report surveyed 1,000 workers in the UK and 1,000 workers in the US at the height of the coronavirus outbreak in April 2020, to reveal how stress, distraction and workplace disruption led to people making mistakes at work. Over half (52%) of employees said they were more error-prone while stressed, while over two-fifths said they made more mistakes when they felt tired (41%) or were distracted (42%). Small wonder, then, that 43% employees reported that they had made mistakes resulting in cybersecurity repercussions for themselves or their company.

When looking at the reason why one in four of respondents admitted to falling for phishing scams, 47% of respondents cited distraction as the main cause, with 57% of workers claiming that they were more distracted when working from home.

More about cybersecurity

- 30 fastest-growing cybersecurity skills to learn in 2021
- Meet the hackers who earn millions for saving the web
- Top 5 programming languages for security admins to learn
- End user data backup policy (TechRepublic Premium)

TESSIAN

Why Tessian?

Solutions

Products

Customers

Resources

Blog

Company

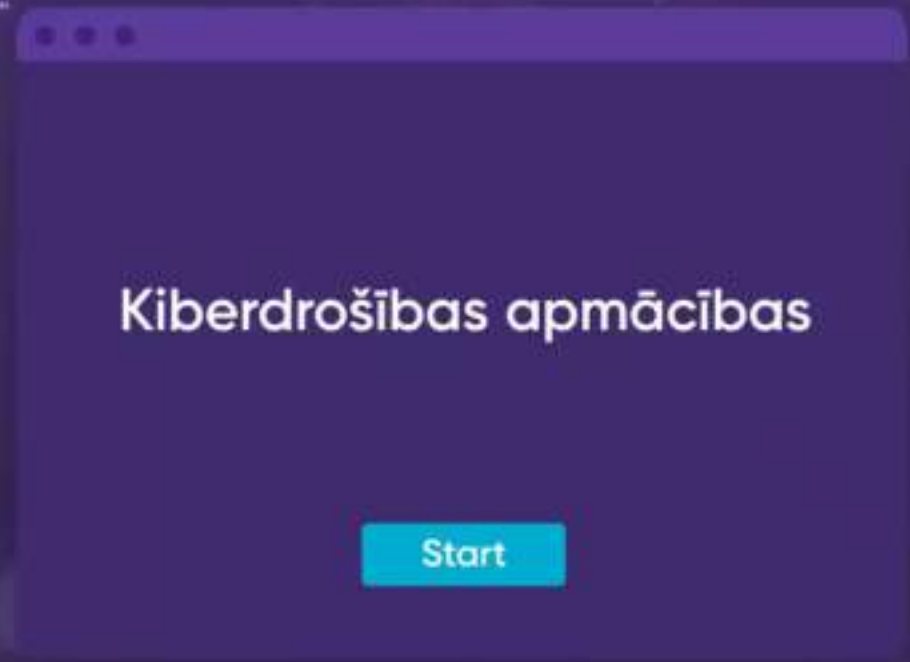
Phishing has been a persistent problem during the COVID-19 pandemic. In April, Google alone saw more than 18 million daily email scams related to COVID-19 in a single week. Hackers are taking advantage of psychological factors like stress, social relationships and uncertainty that affect people's decision-making. Here's a look at some of the psychological factors that make people vulnerable and what to look out for in a scam.

"More than half (52%) of those in our survey said that stress causes them to make more mistakes."



Kā pasargāt savu uzņēmumu no kiberdraudiem,
ko rada uzbrukumi gala lietotājiem ?

2. Apmācīt darbiniekus



Kiberdrošības apmācības

Start

Visefektīvāk ir īstenot e-apmācības



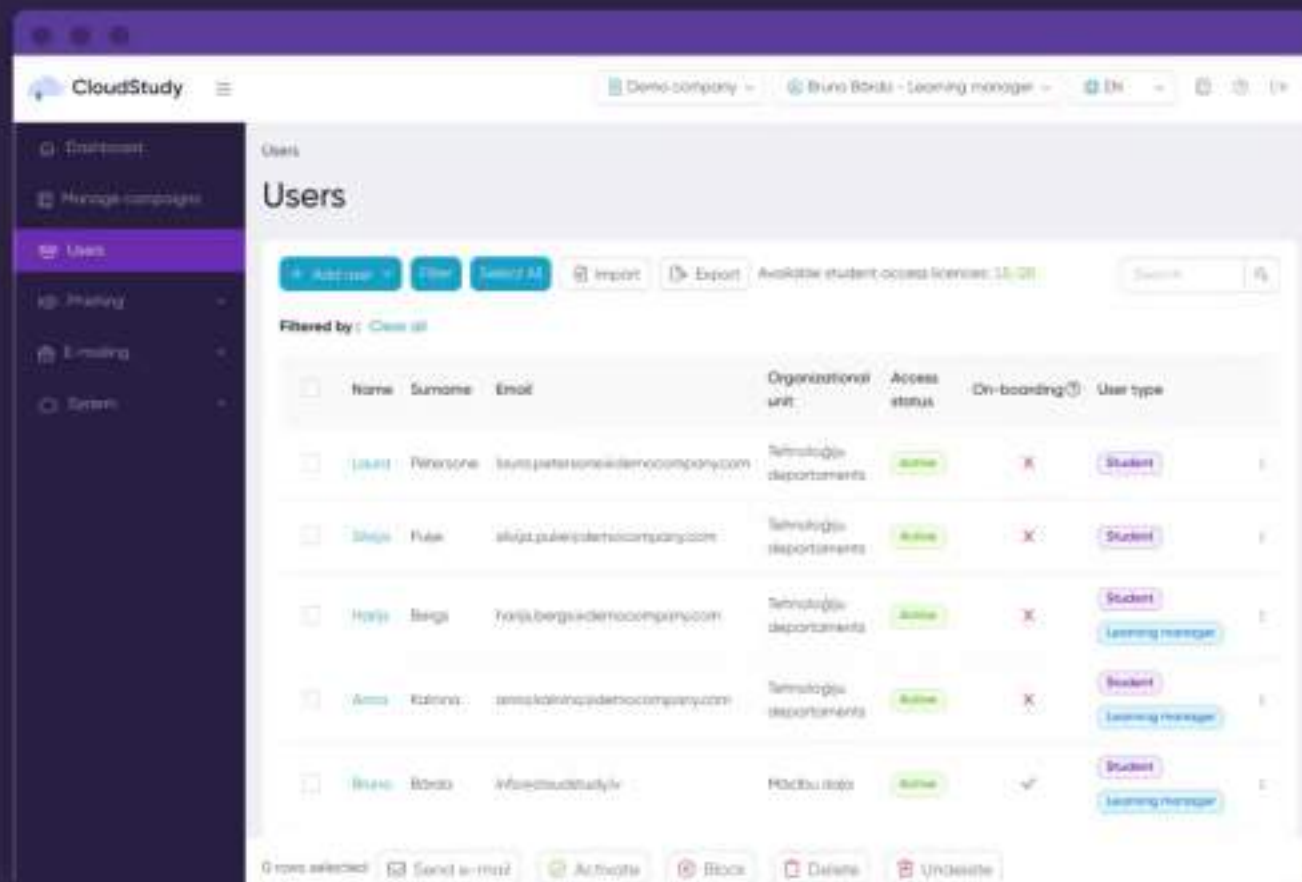
Efektivitāte
(Brandon-Hall Study)



Izmaksas
(SyberWorks)



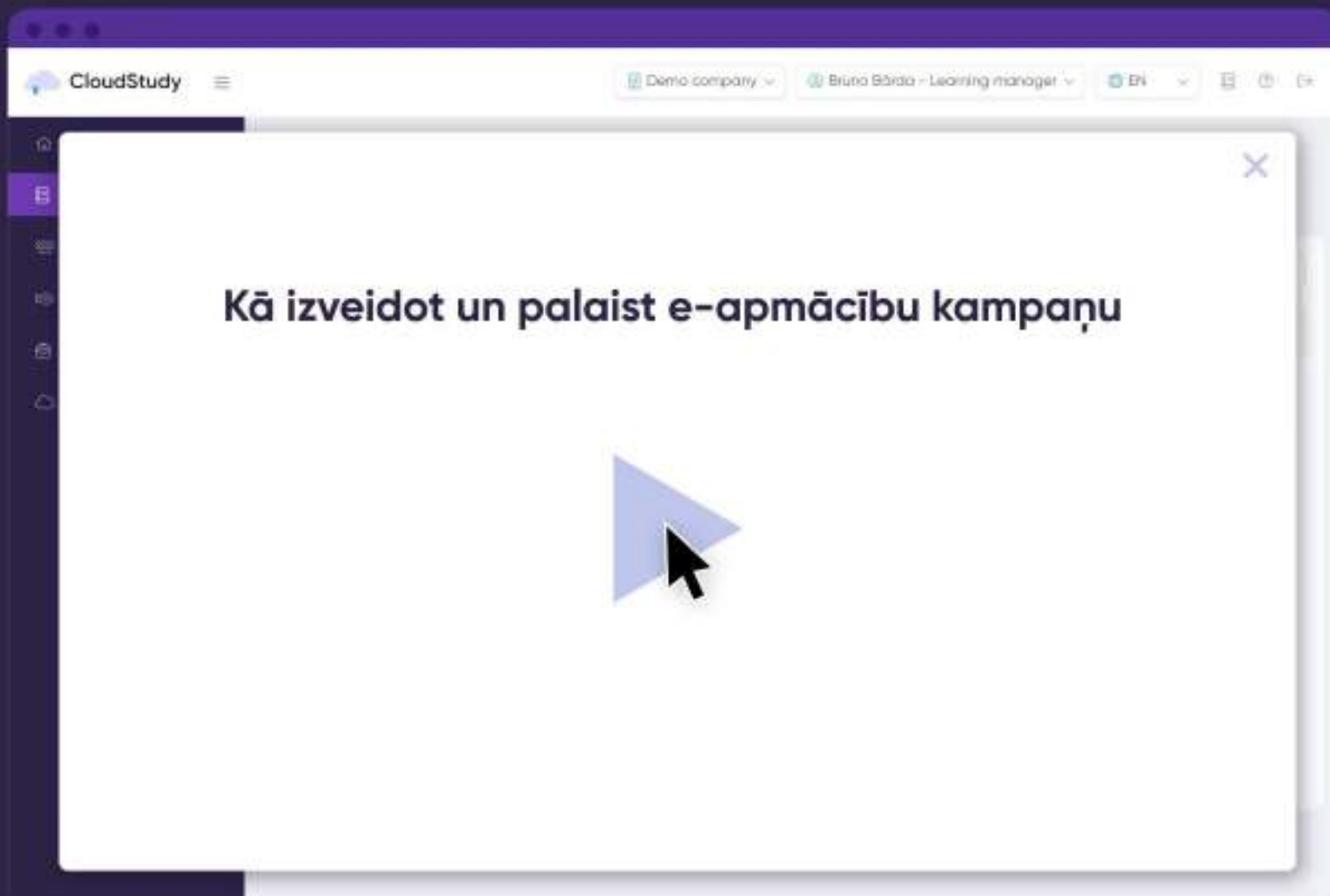
Ātra ieviešana un plūstoša lietotāju pieredze

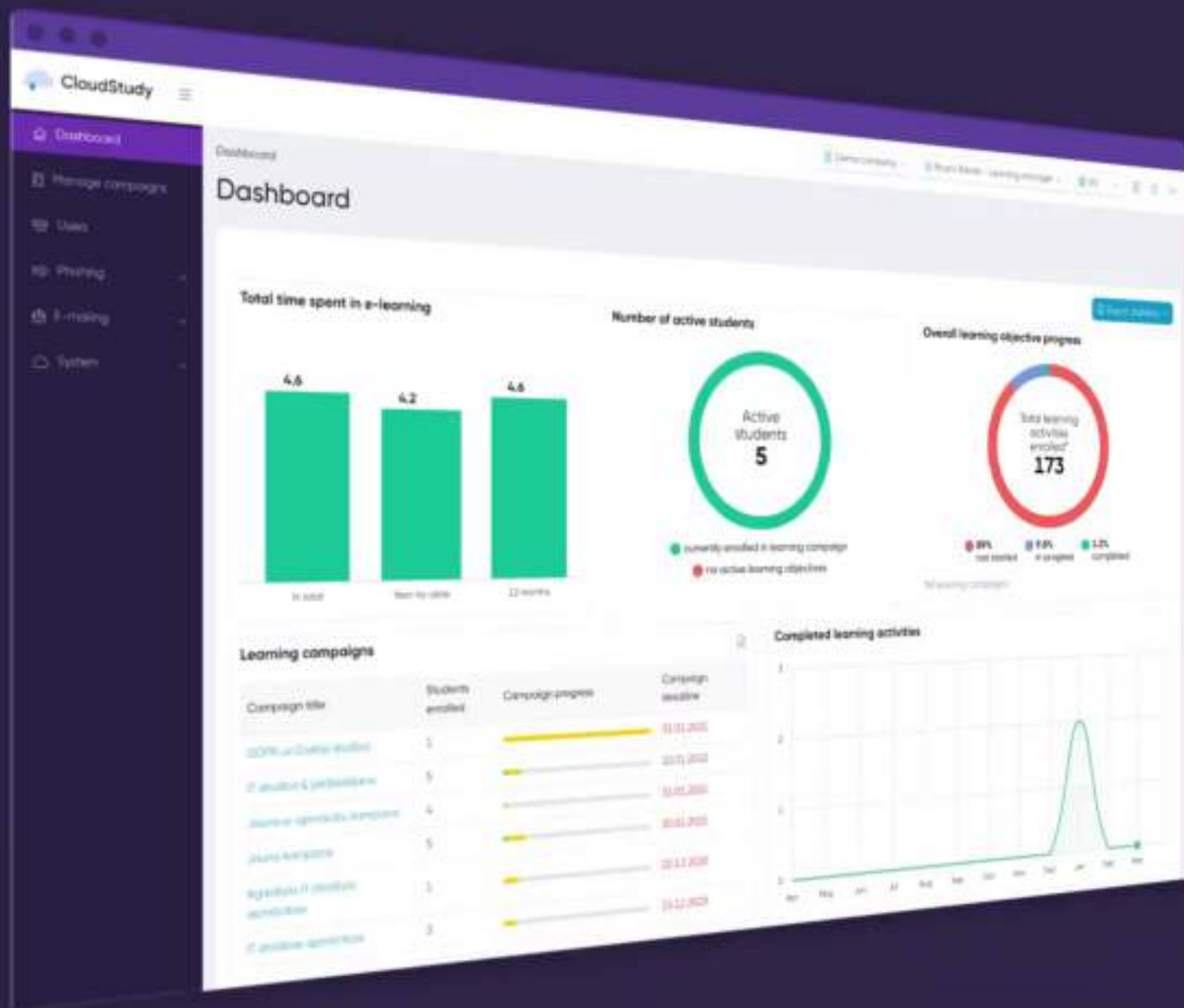


The screenshot shows the 'Users' management page in the CloudStudy application. The interface includes a sidebar with navigation options like 'Dashboard', 'Manage campaigns', 'Users', 'Pruning', 'Emailing', and 'System'. The main content area is titled 'Users' and features a table of user records. Above the table, there are controls for adding users, filtering, and searching, along with an indicator for available student access licenses. The table columns include Name, Surname, Email, Organizational unit, Access status, On-boarding, and User type. At the bottom, there are action buttons for 'Send to mail', 'Activate', 'Block', 'Delete', and 'Unsubscribe'.

<input type="checkbox"/>	Name	Surname	Email	Organizational unit	Access status	On-boarding	User type
<input type="checkbox"/>	Jakob	Petersone	jakob.petersone@democompany.com	Technology departments	Active	X	Student
<input type="checkbox"/>	Steph	Pule	steph.pule@democompany.com	Technology departments	Active	X	Student
<input type="checkbox"/>	Halle	Berg	halle.berg@democompany.com	Technology departments	Active	X	Student Learning manager
<input type="checkbox"/>	Anna	Kalins	anna.kalins@democompany.com	Technology departments	Active	X	Student Learning manager
<input type="checkbox"/>	Bruno	Baldi	bruno@cloudstudy.fr	MOCKU000	Active	✓	Student Learning manager

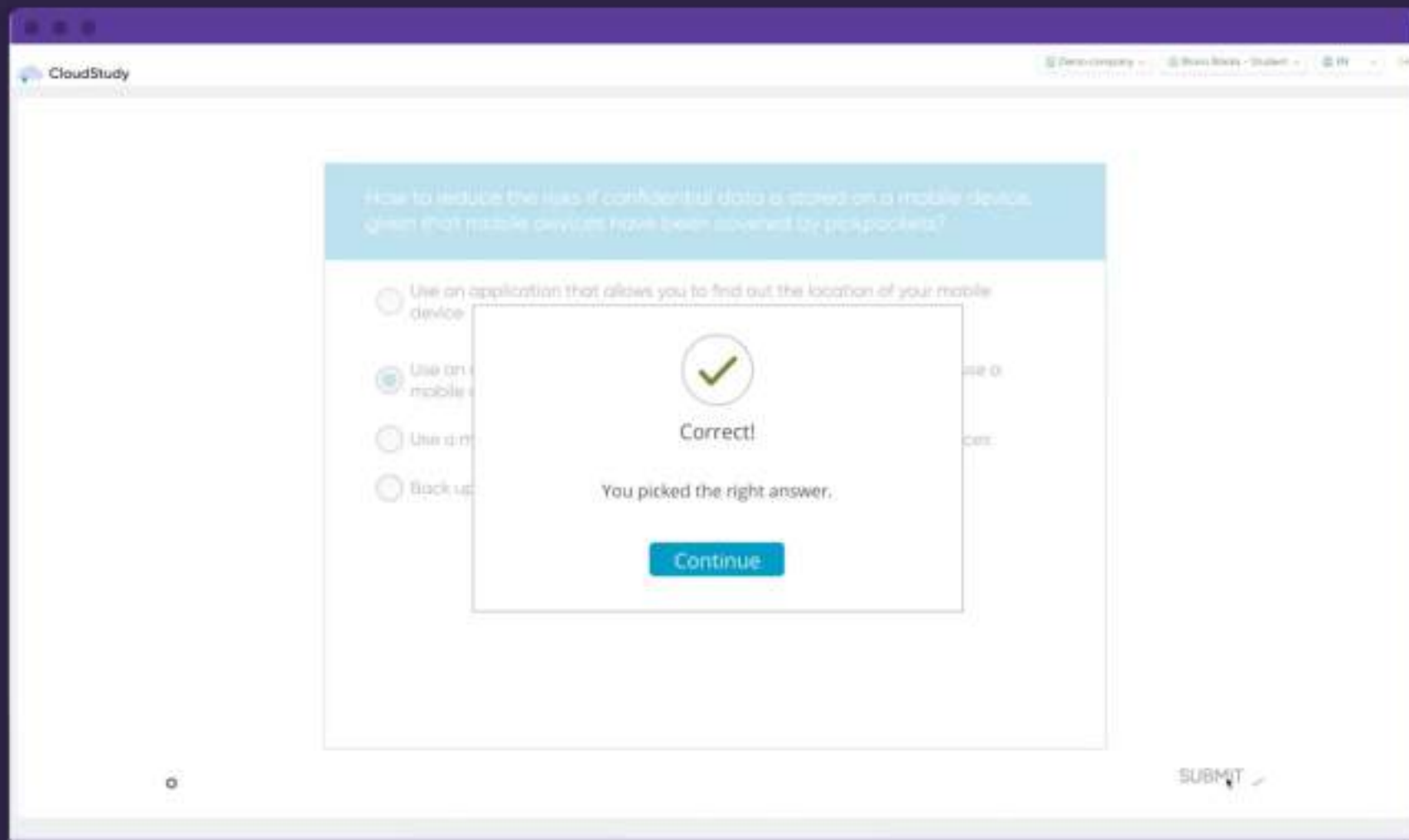
Detalizēti lietošanas pamācības video





Vienkārši lietojama saskarne

Atraktīvs un iesaistošs e-apmācību saturs



The screenshot displays a web browser window with the CloudStudy logo in the top left and navigation links in the top right. The main content area features a quiz question: "How to reduce the risks if confidential data is stored on a mobile device, given that mobile devices have been covered by pickpockets?". Below the question are four radio button options. A central modal window is overlaid on the options, indicating a correct answer. The modal contains a green checkmark icon, the text "Correct!", and "You picked the right answer." Below this is a blue "Continue" button. In the bottom right corner of the page, there is a "SUBMIT" button with a checkmark icon.

CloudStudy

Democrazia - Home Study - Student - IT

How to reduce the risks if confidential data is stored on a mobile device, given that mobile devices have been covered by pickpockets?

- Use an application that allows you to find out the location of your mobile device
- Use an application that allows you to find out the location of your mobile device
- Use an application that allows you to find out the location of your mobile device
- Back up

Correct!

You picked the right answer.

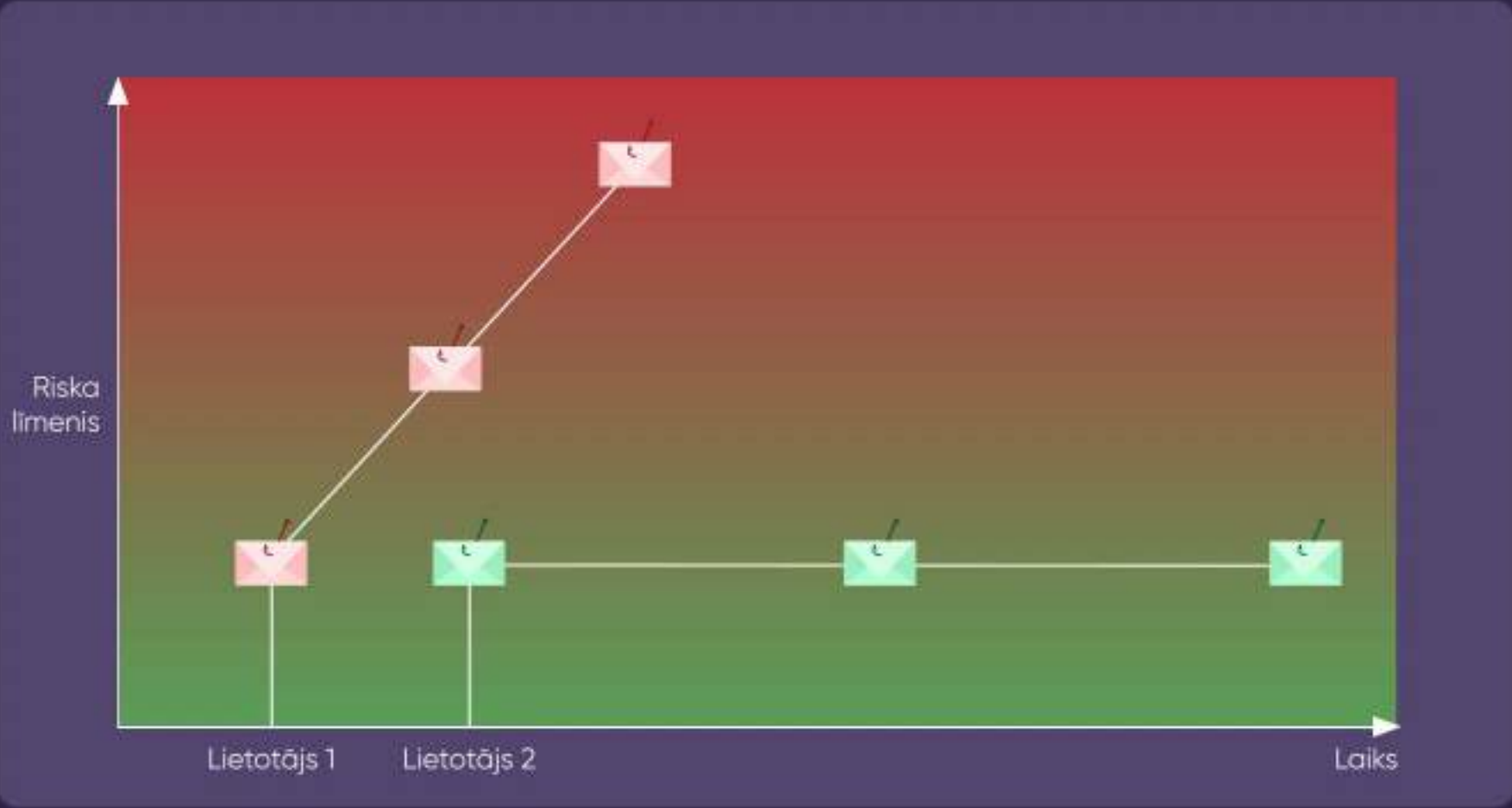
Continue

SUBMIT ✓

Pikšķerēšanas simulācijas palaišana ar dažiem peles klikšķiem

Smart dePhish:





Phishing simulations

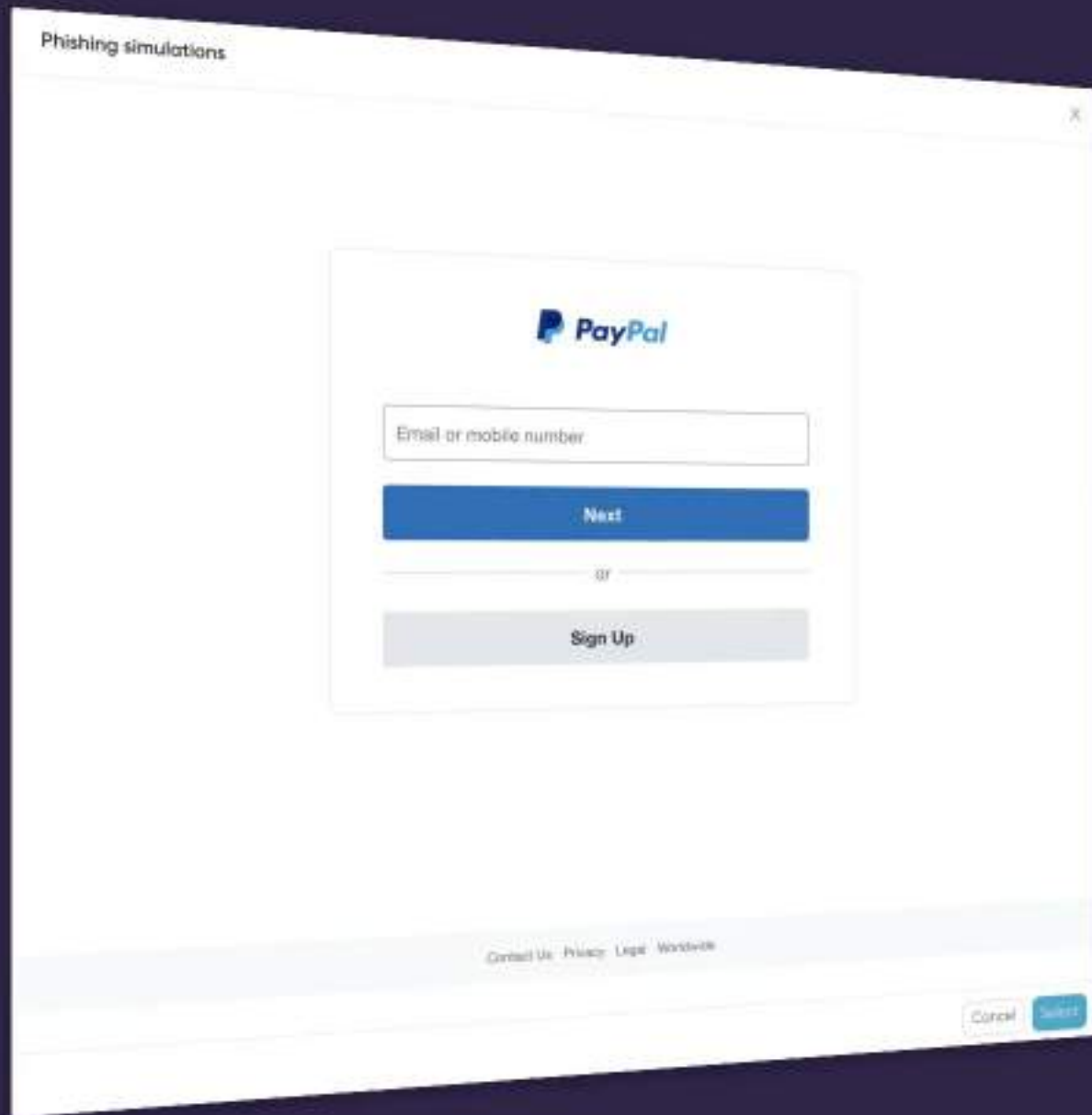
Phishing simulation scenario	Difficulty	Supported languages	Preview e-mail template	Preview landing page
Microsoft Office 365 izīrta parole atjaunināšana	MEDIUM	LV	W	W
Google Chrome tīmekļa pārlūka drošības iestāžu piegāde	MEDIUM	LV	W	W
UPS: Jums drīz tiks piegādāts sūtījums	HIGH	LV	W	W
OMNIVA: Pārdošanas sūtījums pakomātā	HIGH	LV	W	W
Conventus: Rīgas satiksmes naudas sadaļas piedāvājums	HIGH	LV	W	W
Paypal: New incoming transaction (ENG)	MEDIUM	LV	W	W
Paypal: You have money in your account	MEDIUM	EN	EN	EN
SPKIC: Identificēti kontakti	HIGH	LV	W	W
VID: Nodaļu atmaksa	HIGH	LV	W	W
Latvijas poste: Jauns atmantojams sūtījums	LOW	LV	W	W

1-10 of 12

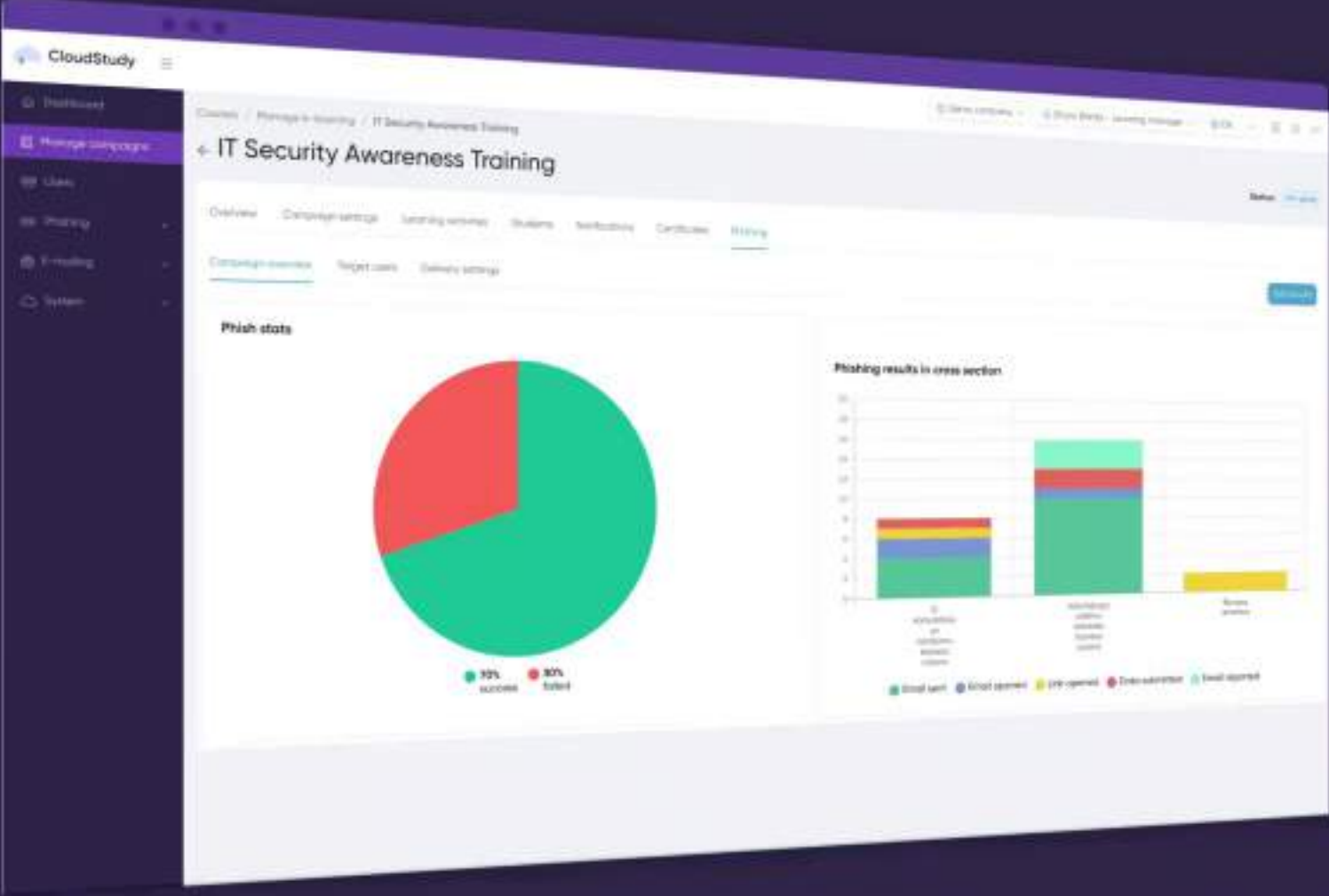
1 2 10 / page Go to

Cancel Select

Plaša pikšķerēšanas
veidņu izvēle



Plaša pikšķerēšanas
veidņu izvēle



Pikšķerēšanas
kampanju analītika

Jebkuru SCORM bāzētu e-apmācību izmitināšana

