IT drošības kultūra: Kas tas ir un kādēļ tas ir nepieciešams katrai organizācijai ?

Imants Felsbergs
Biznesa attīstības vadītājs

Corporate Solutions

Datu incidentu seku novēršanas vidējās izmaksas, 2020

Ponemon Institute*

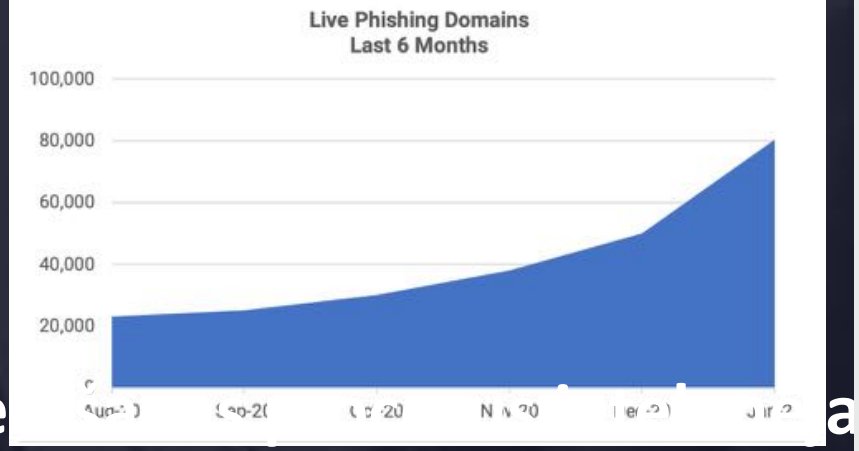
90% datu incidentu pēdas ved pie gala lietotāju pikšķerēšanas uzbrukumiem

(Verizon)

Pandēmijas apstākļos pikšķerēšana ir saasinājusies vēl vairāk!

Kā pikšķe a

In 2020 phishing exploded as the world faced a 100-year pandemic and many people moved to remote working and learning, which changed the phishing threat landscape forever. Our recent report, The State of Phishing, SlashNext Threat Labs, reports on the latest statistics and trends in phishing. In the last 12 months, cybercriminals launched thousands of new phishing pages every hour to harvest personal information, steal corporate data, and commit credit card fraud with no sign of slowing down. Phishing increased 42% in 2020, over 2019. By mid-2020, SlashNext Threat Labs saw the number of daily phishing threats top 25,000 a day, a 30% increase over 2019 figures. By fall, the number had grown to 35,000/day and grew to 50,000/day by December and continues to rise in 2021.



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 5G Developer COVID-19 More Newsletters Forums Resou

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.

More about cybersecurity

- 10 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)

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.

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

Visefektīvāk ir īstenot e-apmācības

Efektivitāte
(Brandon-Hall Study)

Izmaksas
(SyberWorks)

IT Drošības kultūra

Definīcija

IT drošības kultūra (angl. Cybersecurity Awareness) **ir organizācijas stāvoklis,** kura ietvaros darbinieki saprot kas ir kiberdraudi, spēj tos identificēt, novērtēt to ietekmi un saprot kā jārīkojas, lai novērstu riskus vai minimizētu potenciālo negatīvo ietekmi.


Inbox - tava.vranda@tovadomena.com

IT Drošības kultūra

Nobriešana

SANS institūta IT Drošības kultūras 5 brieduma līmeņi.

IT Drošības kultūra

Nobriešana

Kurā brieduma līmenī ir Jūsu organizācija?

SANS institūta IT Drošības kultūras 5 brieduma līmeņi.

Paldies par uzmanību

Vēlies uzzināt vairāk? Raksti mums!

CloudStudy

Imants Felsbergs
Biznesa attīstības vadītājs
Imants.Felsbergs@csolutions.lv

Corporate