Are your customers one wrong click away from a data breach?

The evolving threat landscape puts businesses of every size at risk. But with the correct knowledge and toolset, your MSP business can capitalize.

What is phishing?

Phishing is a type of online fraud aimed at stealing data and cash. It's a harmful and widespread threat that sees bad actors attempt to extract private information like login credentials from their victims. While attacks usually begin with mass emails containing links to fake websites, new vectors such as vishing (voice phishing) are gaining popularity. Phishers can use practically any communication and data sharing platform to distribute their phishing links, with social networks, online stores and mail services all commonplace.

Advanced phishing that targets specific individuals is known as spear phishing (or whaling when an especially high-profile individual is targeted). These types of attack see the perpetrator deploy social engineering, a form of digital coercion based on publicly available information, to persuade people to transfer them money.

See how a phishing attack cost one boutique hotel $1 million[1]

Phishing risks

Phishing attacks can harm businesses of every size and industry. A **data breach** is possible if an employee unwittingly compromises customer data, which, depending on the type of data involved, can incur heavy fines. Phishing websites themselves may contain malware that sabotages an organization's systems, causing **downtime** and **monetary loss**. And while a business's tolerance to downtime will depend on its operating model, the impact on "always on" public services, such as hospitals, can be drastic.

Phishing emails and websites today look more authentic than ever before, so even experienced users can be fooled. Implementing strong defenses and a cybersafe culture is therefore crucial for businesses – and for you, it's a **market opportunity**.

The global average cost of a data breach was $4.45 million in 2023[2]

If you have any questions, please contact us at msp@kaspersky.com.

Countering phishing to secure your clients

Phishing is not something that you can stop altogether – bad actors will always target businesses in their bid to make a quick buck. You can, however, assist your clients in fostering a culture of cybersafety through **continuous online education**. You can also ensure that they have **best-in-class endpoint protection**, so that when a mistake is made, they don't have to pay the price.

Clients to approach

All business are vulnerable to phishing attacks, with attempted attacks rising 40% from 2022 to 2023.[3] However, small-to-medium sized businesses (SMBs) are at the greatest risk, as they may lack both security awareness **and** defensive capability, whereas enterprises are likelier to at least boast the latter. A data breach can also be especially severe for small businesses, as they may be unable to recover financially.

"I want to know that if one of my employees clicks a malicious link, we aren't going to lose money – that the damage isn't irreversible."

The solution: Kaspersky endpoint protection and cybersecurity training

You can mitigate your clients' risk from phishing and malware with the continuously updated protection in **Kaspersky Endpoint Security Cloud**, which SMB users love for its light weight and usability. And trust us when we say it's reliable: our protection was awarded **680 first place finishes** (more than any competitor) in independent tests between 2013 and 2023.

Your clients can also use KES Cloud to continuously upskill employees with training activities that improve the business's security hygiene and reduce the likelihood of a successful phishing attack. These modules are available on demand, so users can develop skills anywhere, anytime. What's more, there's even specialist phishing training for advanced IT specialists!

To learn more about managing your clients' risk with Kaspersky solutions, email us at msp@kaspersky.com or click below.

Find out more

1. NIST. (2020). Hotel CEO Finds Unwanted Guests in Email Account. NIST.
2. IBM. (2023). Cost of a Data Breach 2023. IBM.
3. Kaspersky. (2024). Kaspersky Reports Phishing Attacks Grow by 40 Percent in 2023. Kaspersky.
4. Kaspersky. (2024). Kaspersky Independent Testing. Kaspersky.

kaspersky