Scammers increasingly distribute spam and phishing emails from legitimate company websites

Kaspersky researchers have identified a growth in the usage of cunning spam and phishing delivery technique. Malicious internet users are increasingly exploiting registration, subscription, and feedback forms on websites to insert spam content or phishing links into confirmation emails from respected and trustworthy companies on a global scale.

Malicious users are constantly looking for new methods to deliver their spam and phishing messages to recipients, while bypassing existing content filters. Ideally, they try to make letters come from a legitimate source with a good reputation so that users cannot ignore the unwanted email. This also creates a challenge for companies as this unwanted spam or even malicious content, seemingly sent on their behalf, could compromise their customers' trust or even lead to personal data leaks.

The method is quite simple and effective. Today, almost every company is interested in receiving feedback from their clients to improve the quality of service, customer retention, and reputation. To do this, companies ask customers to register a personal account, subscribe to newsletters or communicate with feedback forms on the website, for example, to ask questions or leave suggestions. These are exactly the mechanisms that attackers are exploiting.

All three mechanisms require the customers' name and email address, so they can receive a confirmation email or feedback. According to Kaspersky researchers, scammers are adding spam content and phishing links into this mail. They simply add the victim's email address into the registration or subscription form and type their message instead of the name. The website will then send a

modified
confirmation letter to that address, containing an advertisement or phishing link at the beginning of the
text instead of the recipient's name.
"Most of these modified letters are linked to online surveys designed to obtain personal data from visitors. Notifications from a reliable source usually pass through content filters with ease, as they are
official messages from a reputable company. This is why this new method of unwanted, yet seemingly
innocent, spam emailing is so effective and worrying," notes Maria Vergelis, security expert at Kaspersky.
To keep companies from possible reputational losses, we advise:
 To check how the feedback forms work on your website
 To embed several verification rules that would cause an error when trying to register a name with inappropriate symbols
 To conduct a vulnerability assessment of the website, if possible.
Read the full text of the report on Kaspersky Daily.

Scammers increasingly distribute spam and phishing emails from legitimate company websites
About Kaspersky
Kaspersky is a global cybersecurity company founded in 1997. Kaspersky's deep threat intelligence and
security expertise is constantly transforming into innovative security solutions and services to protect
businesses, critical infrastructure, governments and consumers around the globe. The company's comprehensive security portfolio includes leading endpoint protection and a number of specialized security solutions and services to fight sophisticated and evolving digital threats. Over 400 million users
are protected by Kaspersky technologies and we help 270,000 corporate clients protect what matters
most to them. Learn more at www.kaspersky.com.