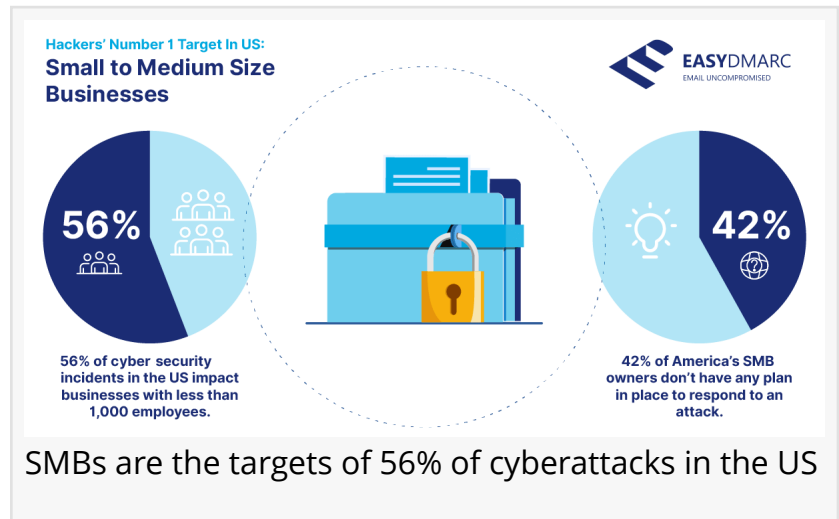# For busy SMB owners and IT staff, EasyDMARC provides a fast solution to understanding their email security risks

Small and medium business are the targets of 56% of incidents in the US. EasyDMARC's domain scanner shows business owners how secure their email ecosystem is.

YEREVAN, ARMENIA, September 20, 2021 /EINPresswire.com/ -- While cyberattacks surge in 2021, a recent study highlights that American small and medium business (SMB) owners remain overconfident about cyber threats. Yet, they are now the prime

SMBs are the targets of 56% of cyberattacks in the US

targets of hackers. For busy SMB owners and IT staff, EasyDMARC provides a fast solution to understanding their email security risks.

In its first half of 2021 report, Accenture Security found that there was a 125% year-over-year increase in incident volume. While most countries and industries were merely touched, the United States was the most severely impacted, targeted by 36% of attacks. This is a threat that SMB owners in America need to know about.

Yet, in its Q3 2021 Momentive Small Business Survey, CNBC reported that 56% of America's SMB owners are not concerned about being targeted by hackers. 42% of them don't have any plan in place to respond to an attack. This overconfidence could explain why hackers from all around the world are targeting American SMBs.

Additionally, in its 2021 Data Breach Investigation Report, Verizon pointed out that the majority of incidents impact American businesses with less than 1,000 employees. SMBs are the targets of 56% of incidents in the US, with a surge in cases more than doubling, from 407 in 2020, to 1037 cases in 2021.

Furthermore, financial losses due to cyberattacks come predominantly through a vital channel for SMBs: their email marketing. This happens via a type of attack, known as business email

compromise (BEC), where a company's emails are being forged. The FBI 2020 Internet Crime Report shows that BEC takes the largest financial toll, counting for $1.8 billion of the $4 billion losses from all forms of hacking.

The reasons for SMBs to overlook their risks toward business email compromise range from focus on the operational side of the business, to lack of time, or resources and staff to handle this issue. EasyDMARC understands the specifics of running an SMB, and provides an online tool to tackle the risks of business email compromise in a matter of seconds, with no technical knowledge needed. The tools and solutions are available to all SMBs, or to the MSPs that support them.

EasyDMARC's [domain scanner](#) shows business owners how secure their email ecosystem is, with a simple tool that anybody can use and understand. The scan provides an immediate report on the status and performance across the 4 main email security protocols (DMARC, SPF, DKIM and BIMI), and provides guidance on how to improve them.

From there, SMB owners, their staff, or their MSPs can quickly understand how secure their email ecosystem is and can take swift and easy action to improve their email security. EasyDMARC's solutions do not require IT expertise to be implemented.

About EasyDMARC

EasyDMARC provides solutions for businesses to ensure their email and direct marketing security in cyberspace, quickly and without expert knowledge. EasyDMARC solutions protect companies against data leakage, financial loss, email phishing attacks, and prevent the unauthorized use of their domain name and email addresses. More information available at https://easydmarc.com/.

Sources
https://www.accenture.com/us-en/blogs/security/triple-digit-increase-cyberattacks
https://www.cnbc.com/2021/08/10/main-street-overconfidence-small-businesses-dont-worry-about-hacking.html
https://enterprise.verizon.com/content/verizonenterprise/us/en/index/resources/reports/2021-data-breach-investigations-report.pdf
https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf

Gerasim Hovhannisyan
EasyDMARC, Inc.
+1 888-563-5277

gerasim@easydmarc.com

This press release can be viewed online at: https://www.einpresswire.com/article/551833761