

Is Email Putting Your Business at Risk?

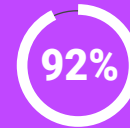
Email is essential to everything businesses do, from internal communications to customer service. But cybercriminals also use email—to steal data, lock users out of their systems, or worse.

270,557

unique phishing email campaigns reported in Q3 alone¹



of data breaches begin with a phishing email²



of all malware comes in by email³

What do attackers want?

76%
of data breaches are financially motivated⁴

39%
of all malware is ransomware¹⁰

58%
of data breach victims are small businesses¹¹

What are phishing emails?

They look like legitimate emails from banks, web services providers, or other organizations, but are designed to trick people into sharing personal information (like login credentials) or downloading malware.

76%
of organizations have experienced a phishing attack⁴

10%
of malicious emails bypass security and land in users' inboxes⁵

Almost **15%**
of emails reported by employees were malicious⁶

4%
of people will click on a phishing email⁷

All it takes is **1** click to put everything at risk

What are some of the most common disguises used by spam and phishing emails?⁸

15.9%
bills or invoices

15.3%
email delivery failure notifications

13.2%
legal notices

11.5%
scanned documents

3.9%
package deliveries

Supporting Microsoft 365? Its default security may not be enough.

You may want to avoid relying solely on the security features built into Microsoft 365™, as cybercriminals can sometimes design attacks specifically to target its massive user base. If something gets through, what's stopping it from infecting the entire IT infrastructure?



53%
of threats detected by Microsoft 365 are phishing emails¹⁴



Microsoft 365 macros account for **45%** of malware delivery mechanisms¹⁵

1,100

internet hostnames with phishing pages mimic Microsoft 365 sign-in screens or notifications¹⁶

Most Often, it's Money

Cybercrime will cost the globe an estimated¹²

\$600 billion

This is the equivalent of¹³

0.8% Global GDP

Want to Enhance Your Email Security?

N-able™ Mail Assure is designed to help businesses fight back against phishing, malware, and other email-related risks. Learn more at n-able.com/products/mail-assure.

N-able empowers managed services providers (MSPs) to help small and medium enterprises navigate the digital evolution. With a flexible technology platform and powerful integrations, we make it easy for MSPs to monitor, manage, and protect their end customer systems, data, and networks. Our growing portfolio of security, automation, and backup and recovery solutions is built for IT services management professionals. N-able simplifies complex ecosystems and enables customers to solve their most pressing challenges. We provide extensive, proactive support—through enriching partner programs, hands-on training, and growth resources—to help MSPs deliver exceptional value and achieve success at scale.

© 2021 N-able Solutions ULC and N-able Technologies Ltd. All rights reserved.

The N-ABLE, N-CENTRAL, and other N-able trademarks and logos are the exclusive property of N-able Solutions ULC and N-able Technologies Ltd. and may be common law marks, are registered, or are pending registration with the U.S. Patent and Trademark Office and with other countries. All other trademarks mentioned herein are used for identification purposes only and are trademarks (and may be registered trademarks) of their respective companies.

¹Phishing Activity Trends Report – 3rd Quarter 2018, "Anti-Phishing Working Group, Inc. http://docs.apwg.org/reports/apwg_trends_report_q3_2018.pdf (Published December 2018, Accessed February 2019).

²2018 Data Breach Investigations Report, "Verizon. <https://enterprise.verizon.com/resources/reports/dbir/> (Published April 2018, Accessed January 2019).

³2018 Data Breach Investigations Report, "Verizon. <https://enterprise.verizon.com/resources/reports/dbir/> (Published April 2018, Accessed January 2019).

⁴2018 State of the Phish, "Wombat Security. <https://www.wombatsecurity.com/state-of-the-phish/> (Published January 2018, Accessed January 2019).

⁵The State of Phishing Defense, "Cofense. <https://cofense.com/state-of-phishing-defense-2018/> (Published October 2018, Accessed January 2019).

⁶Enterprise Phishing Resiliency and Defense Report, "Cofense. <https://cofense.com/phishing-resiliency-report-2017/> (Published 2017, Accessed February 2019).

⁷2018 Data Breach Investigations Report, "Verizon. <https://enterprise.verizon.com/resources/reports/dbir/> (Published April 2018, Accessed January 2019).

⁸Internet Security Threat Report, Vol. 23, "Symantec. <https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-2018-en.pdf> (Published March 2018, Accessed January 2019).

⁹2018 Data Breach Investigations Report, "Verizon. <https://enterprise.verizon.com/resources/reports/dbir/> (Published April 2018, Accessed January 2019).

¹⁰2018 Data Breach Investigations Report, "Verizon. <https://enterprise.verizon.com/resources/reports/dbir/> (Published April 2018, Accessed January 2019).

¹¹2018 Data Breach Investigations Report, "Verizon. <https://enterprise.verizon.com/resources/reports/dbir/> (Published April 2018, Accessed January 2019).

¹²Economic Impact of Cybercrime—No Slowing Down, "Center for Strategic and International Studies. <https://www.csis.org/analysis/economic-impact-cybercrime> (Published February 2018, Accessed February 2019).

¹³Economic Impact of Cybercrime—No Slowing Down, "Center for Strategic and International Studies. <https://www.csis.org/analysis/economic-impact-cybercrime> (Published February 2018, Accessed February 2019).

¹⁴Microsoft Security Intelligence Report, Vol. 23, "Microsoft. https://info.microsoft.com/rs/157-GQE-382/images/EN-US_CNTNT-eBook-SIR-volume-23_March2018.pdf (Published March 2018, Accessed January 2019).

¹⁵The State of Phishing Defense, "Cofense. <https://cofense.com/state-of-phishing-defense-2018/> (Published October 2018, Accessed January 2019).

¹⁶Malware Review 2018, "Cofense. https://cofense.com/wp-content/uploads/2018/03/Cofense_Malware-Review_2018.pdf (Published March 2018, Accessed January 2019).