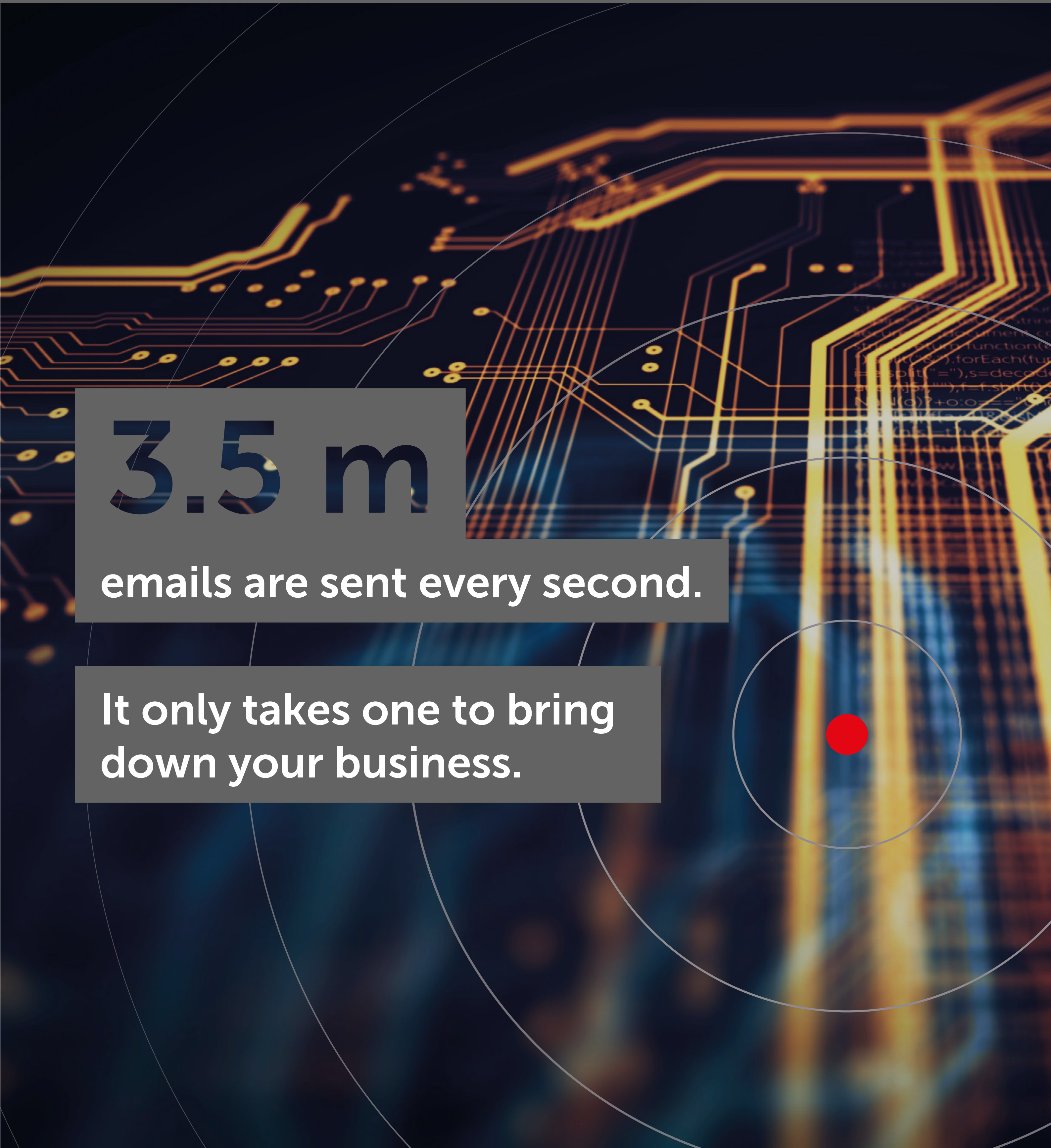
Kaspersky for Business

Kaspersky Security for Microsoft Office 365



3.5 m

emails are sent every second.

It only takes one to bring down your business.

Moving to the cloud? Secure it.

With more than 100 million monthly users, Microsoft Office 365 is officially more popular with business users than its traditional, on-premises counterpart[1].

But lightening the load on infrastructure and resources doesn't reduce cyberthreats, especially when it comes to Office 365 email.

Spam, malicious attachments, phishing (including spear phishing/business email compromise BEC), ransomware and data theft are just as big a problem for Office 365 mail as they are on-premises.

And what about the resources they consume? From pressure on bandwidth to lost productivity, spam continues to clog the arteries of businesses the world over: more than half of all global email traffic is spam.

For small and medium-sized businesses, keeping communications flowing and cyberthreats and productivity vampires out is a big challenge.

⇧ **+600%** Increased in 2016, of Malware targeting Microsoft Office 365[2]

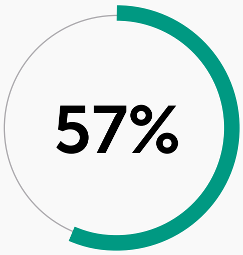
How to click start a cyberattack

You know the drill: Email is the number one malware vector threatening business security[3].

So why do your users keep clicking?

Despite your best efforts, one in two will click on an unsolicited mail – even though 78% say they understand the risks[4].

No wonder it's the tool of choice for cybercriminals; the quickest route to the heart of your business is the end-user's inbox. And when cybercriminals tailor the mails to look legitimate, it's harder than ever to detect and block them, never mind stop users from clicking.



of Microsoft Office 365 users had at least one copy of the spam-based Cerber ransomware attack in their inboxes in 2016[5].

[1] *Satya Nadella, Microsoft Q3 2017 earnings call. In 2017, Microsoft Office 365 license sales outstripped the on-premises version for the first time.*

[2] *https://redmondmag.com/articles/2017/06/01/office-365-security.aspx*

[3] *Verizon Data Breach Investigation Report 2017*

[4] *Friedrich-Alexander Universitat: https://www.fau.eu/2016/08/25/news/research/one-in-two-users-click-on-links-from-unknown-senders/*

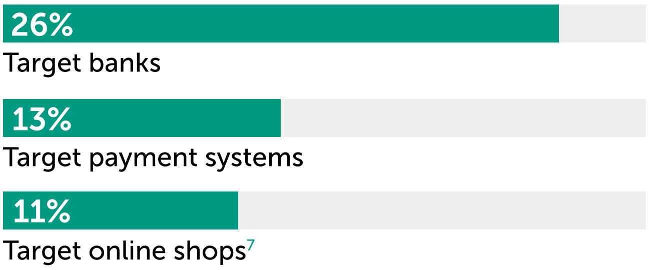
[5] *https://www.scmagazine.com/microsoft-office-365-hit-with-massive-cerber-ransomware-attack-report/article/529295/*

Something phishy?

Most businesses have put time into educating users on the threat of dodgy email.

But what can you do when cybercriminals work around this by targeting specific departments and users with mails tailored to look like they come from the boss, the supplier or a job applicant?

Twenty-one per cent of incidents reported involve some form of phishing[6] and more than half of all attacks target the financial sector:



Phishing attacks usually involve larger scale attempts to steal passwords, banking details, credit card numbers or spread malicious code such as ransomware on the victim's computer. They usually look 'normal' – at a glance – and are sent in large numbers, to broaden the chance of a single person being duped. Before you think you're too smart to be caught out, think about it:

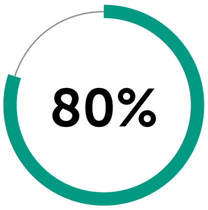
Someone in the accounts department receives an 'URGENT INVOICE FINAL NOTICE' email towards the end of the month. They're busy, it looks legit and it's a PDF attachment, something they're used to seeing in email. So they click. ..And malware is launched.

"How did that happen?"

Because they were in a hurry, the user didn't notice that the file ended in '.exe' – after the more familiar '.pdf'. Or maybe they did look – but the cybercriminals hid the extension from casual view (called 'extension spoofing'). Sometimes, it's as simple as forgetting to change a Windows setting that hides file extensions by default.

Whatever way you look at it, blocking those mails from arriving into your end users' inbox could save your company a lot of trouble. Real file type recognition and attachment filtering by extension are just two security technologies that can help detect and block files masquerading as harmless or legitimate attachments.

> **In Windows, disable the "Hide extensions for known file types" option in the "Folder Options" section of the control tab. This will make it easier for users to spot a file that isn't what it seems.**



of data breaches involve stolen or weak passwords, most of them acquired via phishing emails[8].

Especially for you: Spear phishing

But what happens when cybercriminals take things to another level and target specific recipients at your company with mails and attachments that look almost exactly like legitimate communications?

Spear phishing can dupe even the most vigilant employee: a 'job application' sent to the specifically named hiring manager – with an email referring to a legitimate job advertisement. Or an invoice sent to the correct person in accounts, referring to a company that legitimately does business with you. Sometimes, even the email address of the sender is 'spoofed' to make it look legitimate, at least at a glance or to a non-technical user. These mails usually carry a malicious attachment or link to a malicious web site, from which an attack can be launched or credentials stolen.

[6] *Verizon Data Breach Investigation Report 2017.*

[7] *Kaspersky Lab: https://www.kaspersky.com/about/press-releases/2017_5000-fold-decrease-in-spam-botnet-mailings)*

[8] *Verizon Data Breach Investigation Report 2017.*

A more recent addition to the phishing family is the 'mail from 'The CEO' sanctioning an urgent transfer of money. Known as 'Business Email Compromise' (BEC), these mails contain a convincing request and a spoofed sender address to make it look like it really has come from the boss. Because they're so finely tailored, these attacks often make it past spam traps – they're not mailed in large numbers and are usually only sent to a couple of well-chosen employees.

With BEC in particular, it's easy to understand why people make a mistake and click. Once again, the best defense is to detect and filter out these mails before they reach your users. Security solutions that enable detection of Microsoft Office files with macros, for example, can increase protection against malicious attachments. The ability to analyze previewed attachments for phishing content adds an extra layer of protection. Meanwhile authorized email support can significantly reduce the chances of a spoofed email making it to the end user. From a web point of view, continually updated databases of malicious and phishing URLs mean that, even if a user does click, the site will be blocked.

> **Before clicking on any link, always check that the URL matches up: e.g. kaspesky.com vs Kaspersky.com. And never enter your password or login details via a button on a mail inviting you to do so – at the bare minimum, visit the legitimate web site yourself first, by typing the address into the browser yourself.**

America's Federal Bureau of Investigation (FBI) says over $2.3bn has been lost to CEO email scams[9]. Among the high profile victims are global firms Mattel, SnapChat and FACC.

[9] *https://krebsonsecurity.com/2016/04/fbi-2-3-billion-lost-to-ceo-email-scams/*

Spam: the productivity vampire

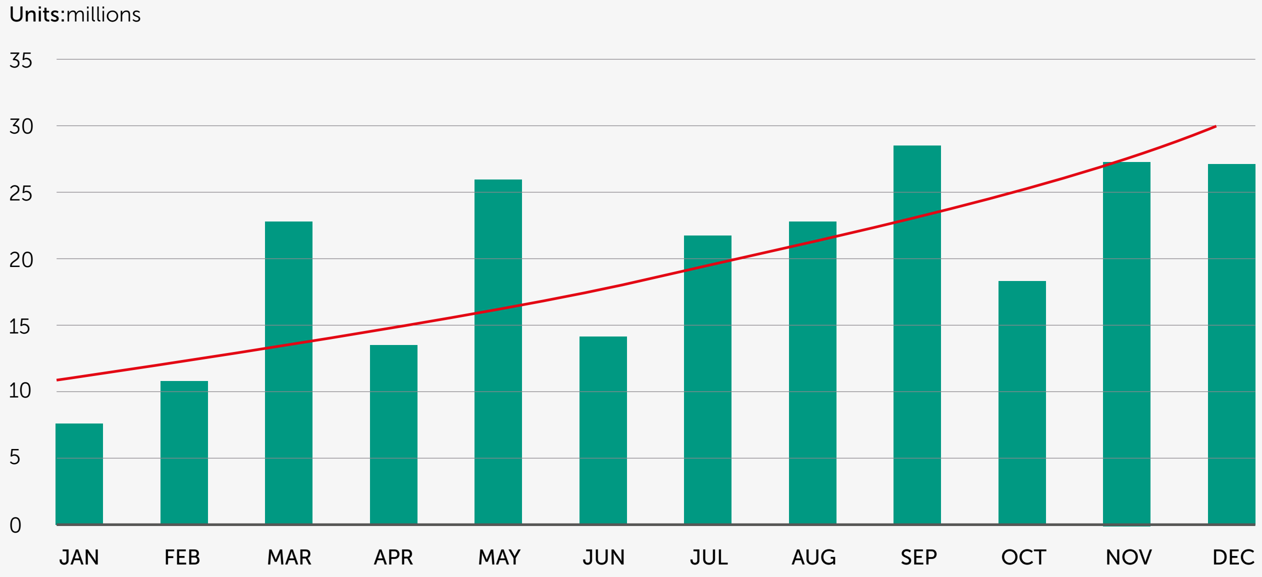
More than 58% of all email traffic is spam[10]. And while a lot of it carries malware, it's also the ultimate productivity and resource thief: the average worker spends 13 hours every year scanning and deleting spam, at an estimated cost of $1250 per year[11]. It's not just wasting employee time, either – more than half of the energy costs of spam are associated with deleting it and searching for legitimate mail[12].

When the time, resources and money you've saved by moving to the cloud are eaten into by junk mail nobody wants, you know you've got a problem.

But what about all the legitimate mail that can go missing because it's mistaken for spam? Thirty-five per cent of business users say blocked legitimate mail has delayed their response to important business 2-3 times in a year; 19% says it's happened 4-6 times[13]. Good anti-spam technology allows easy custom tagging of possible junk messages, improving productivity by filtering away potentially useful mail but not deleting it.

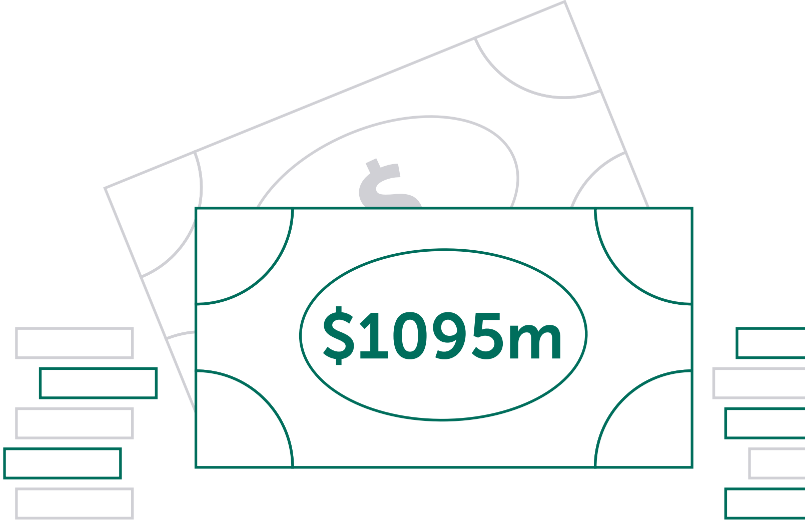
Blocked business mail wastes time, but it's even worse when legitimate mail is automatically deleted, before the administrator or end user gets a say, wasting time and resources insearching - or duplicating - work.

Kaspersky Research shows a massive increase in the volume of malicious spam in 2016



[10] *Kaspersky Security Bulletin: Spam and Phishing in 2016.*
[11] *Source: Atlassian, Time Wasting at Work*
[12] *http://www.brighthub.com/environment/green-computing/articles/33434.aspx*
[13] *https://techtalk.gfi.com/survey-spam-email-disrupts-two-thirds-of-businesses-each-year-infographic/*

Spoof the spoofer: Not sure about a website that looks legitimate but is unexpectedly prompting you to enter a password? Make one up – the real site will reject it. Even better, look for the 'https' prefix on the site URL, indicating that it's secure. A site with no https should give rise to suspicion, especially if it's a financial or ecommerce site.



The spam market is worth an estimated $1095m annually[14].

Malware: the threat at the heart of it all

While many cybercriminals are focused on stealing credentials or duping users into making payments, it's worth remembering that 66% of all malware is installed via malicious email attachments[15]. Ninety-five percent of phishing attacks leading to a breach were followed by some form of software installation[16].

But you've educated your end users and activated the security that shipped with your Office 365 installation, how did this happen?

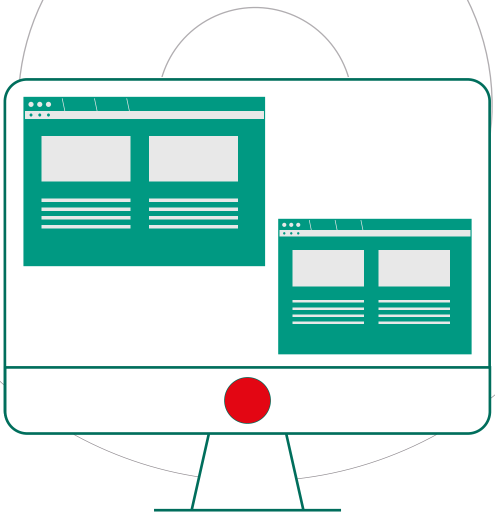
Few criminals are as persistent as cyber criminals. They're always looking for new ways to evade detection and for new vulnerabilities in popular software they can exploit before they can be fixed.

Those vulnerabilities are called 'zero-day' – they're dangerous gaps in software that have just been discovered, but for which there's not yet any protection.

These evolving, often unknown and advanced threats are best countered with security technology that uses machine learning and constantly updated threat intelligence. Together, these ensure that your security is always learning from the threat models it analyses – and from what's happening in the real world of attacks.

Ultimately, it means that rock-solid anti-malware detection and mitigation technology is a core component of securing email, alongside the threats we've just seen such as spam and phishing.

[14] *Kaspersky Lab, Securelist.*
[15] *Data Breach Investigation Report 2017*
[16] *Data Breach Investigation Report 2017*



→← When Office 365 meets cyberthreat 24/7

When it comes to protecting your Microsoft Office 365 mail, the best strategy is making sure the threats are detected and blocked before they can become a problem.

> **Install Kaspersky Security for Microsoft Office 365. It combines next-generation anti-malware with industry-leading anti-spam and anti-phishing to protect your email and end-users from known, unknown and advanced threats.**

To really be effective, you need to be able to do this without slowing down or accidentally deleting legitimate mail traffic. You need to keep the communications flowing – and the cyberthreats out. And if you're really proactive, you can use the information you gain from the blocked threats to gain insight into the type of threats your business is facing.

Kaspersky Security for Microsoft Office 365 is designed specifically to do this for your business. Like your Microsoft Office 365, it's hosted in the cloud. And like all Kaspersky Lab solutions, it's built on the world's most tested, most awarded security[17].

Kaspersky Security for Microsoft Office 365 uses advanced heuristics, sandboxing, machine learning and other next-generation technologies to protect email from ransomware, malicious attachments, spam, phishing and unknown threats.

It also manages false positives more effectively: administrators have complete control over what happens to suspicious mail. Deleted mails are placed in backups that are easily searched and restored. Our 99%+ spam detection rate means your users will spend less time managing useless and potentially dangerous, junk mail.

And because we know you're in the cloud for convenience, resource efficiency and cost-effectiveness, Kaspersky Security for Microsoft Office is easy to use: a single management console takes take care of everything, including a single view of detected threats and statistics. No need for additional hardware or training, no distributive to install.

Discover how our next-generation security technologies can make your Microsoft Office 365 mail even easier to secure and manage

[17] *In 2016, Kaspersky Lab products participated in 78 independent tests and reviews. Our products were awarded 55 first places and 70 top three finishes. https://www.kaspersky.co.uk/top3*