

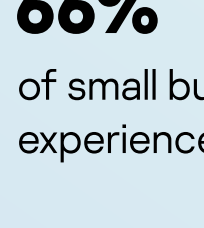
Biggest cyberthreats and challenges for very small businesses



In 2019



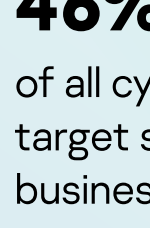
63% experienced a data breach¹



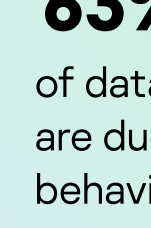
66% of small businesses experienced a cyberattack¹

¹ Ponemon 2019 State of Cybersecurity in Small & Medium Size Businesses

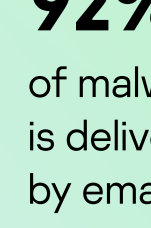
Key statistics to keep in mind



46% of all cyberattacks target small businesses²



63% of data breaches are due to insider behavior³



92% of malware is delivered by email³

² Verizon 2019 Data Breach Investigations Report

³ Purplesec Ultimate List Of Cyber Security Statistics for 2019

Phishing emails... as old as the Internet

Posing as a trusted source, phishing attacks trick users into opening malware-containing links.

But still threat No. 1

Spear phishing – the most widely used infection method employed by hacker groups.⁴

⁴ Symantec 2019 Internet Security Threat Report

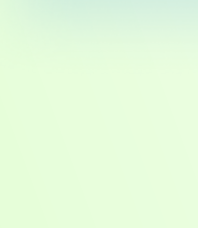
Small businesses kept falling for them! Why?

They're now sophisticated, persuasive, targeted and come at you in different guises. And because the weakest link in your business security is...YOU!

91% of successful data breaches result from phishing emails⁵

⁵ Purplesec Ultimate List Of Cyber Security Statistics for 2019

So what forms of phishing are out there?



Spear phishing
Bespoke emails 'grooming' well-researched victims.



Whaling
Targeting high-level employees with 'urgent & relevant' email requests.



Business Email Compromise (CEO fraud)
Email instructions from the 'boss' (e.g. to transfer funds).



Smishing
Targeting victims with 'compelling' smartphone text messages (e.g. shortcodes).



How to prevent a breach from a phishing email?

- 1 Train ALL your staff on how to identify phishing emails.
- 2 Then train them again.
- 3 And again.

Ransomware: the No. 2 threat

Ransom malware encrypts all your files, then demands a ransom to unlock them. An attack can kill your small business.

Ransomware in numbers

62% of ransomware attacks targeted small businesses in 2019⁶

17% of small businesses, who paid ransom, recovered only some of their organization's data⁷

⁶ Beasley Breach Briefing 2020

⁷ Help Net Security: 46% of SMBs have been targeted by ransomware, 73% have paid the ransom

60% of small businesses plan to pay for return of data after a ransomware attack⁷

Ransomware is delivered when YOU...



Click on a suspicious link or open an email attachment (sounds familiar?).



Visit a compromised website triggering a drive-by-download of a malicious payload.



Download cracked versions of software: online games, adult content etc.

Ransomware variants Cyber Extortion & Sextortion

How do attackers extort money? They threaten to disclose 'compromising' private video footage, photos or text messages publicly, e.g. on social media platforms.

Sextortion in numbers

792,000 attempts worldwide

Victims pay out \$540 on average to stop disclosure⁸

⁸ Digital Shadows: A Tale of Epic Extortions – How Cybercriminals Monetize Our Online Exposure

Impacting 89,000 recipients



Stop ransomware in its tracks

- 1 Install quality endpoint protection including web and email protection.
- 2 Do regular offline backups to make sure all key data can be reliably restored.
- 3 Train all users to spot forms of ransomware delivery.

Cryptojacking – a fluctuating cyberthreat

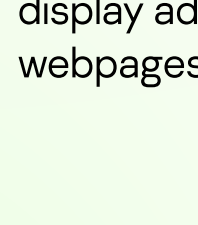
What is it?

Hackers hijack and inject mining script into as many devices as possible to use their CPU power to mine cryptocurrencies.

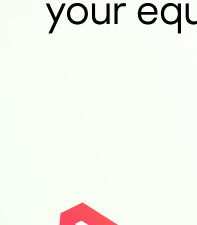
Why fluctuating?

Depends entirely on cryptocurrency value. The higher the value, the more profitable cryptojacking becomes.

How is the mining code script downloaded to your device?



Web browser mining – hackers inject script into display ads or webpages.



Insider mining – employees launch mining programs on your equipment.



You guessed! Phishing (in all its forms).



Cryptocurrency cyberattacks in numbers

4.32% of all Monero coins in circulation were mined using malware⁹

32% of all cyber attacks in the first six months of 2018¹⁰

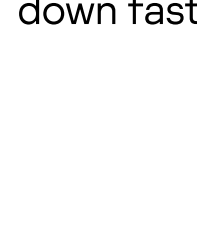
450% increase in cryptojacking during 2018¹¹

⁹ CoinDesk: Crypto Mining Malware Has Netted Nearly 5% of All Monero

¹⁰ Skybox Security Vulnerability and Threat Trends 2018 Mid-Year Update

¹¹ IBM X-Force Threat Intelligence Index 2019

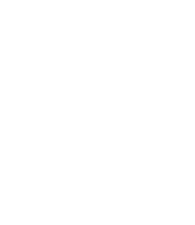
You won't know about it, so what to look out for?



Frequent overheating (your equipment breaks down faster).



Constantly slower response times slows all your business processes.



High processor usage & faster battery drain.

Best remedy? Prevention

- 1 Install an ad-blocker extension for your web browsers.
- 2 Get a security solution that detects cryptomining on your equipment.

And the BIGGEST challenges for Very Small Businesses?

Mobile devices, IOT and BYOD (Bring Your Own Device). Your weakest link and your hardest security challenge.

Mobile malware threats in numbers

56% see mobile devices as the most vulnerable endpoints and entry points to networks¹²

67,500 unique users were attacked on personal data stored on mobile devices¹³

¹² Ponemon 2019 State of Cybersecurity in Small & Medium Size Businesses

¹³ Kaspersky Securelist: Mobile malware evolution 2019 report



24,000 malicious apps are blocked each day¹⁴

Whoops... can't find your smartphone

It usually turns up... right. But what if it's lost or data encryption? Hackers will access your data and your company network.

Think mobile device means smartphone... think again

Card readers... connected cameras, coffee makers, mobile card readers... Your small business secured all entry points from breach? Maybe not...

Any malicious app you download can...

Gain access to your device's memory & data storage, spy on your activity, compromise the entire network you access.

Open internet like the open sea – unpredictably dangerous.

But 69% of us still connect mobile devices to public Wi-Fi¹⁵

¹⁵ NortonLifeLock: 2019 Cyber safety insights report



Keeping mobile devices protected ain't so hard

- 1 Use a strong password and two-factor authentication.
- 2 Update all devices with latest software and security patches.

A headache called Password Management

All password-protected accounts are doors to your business.

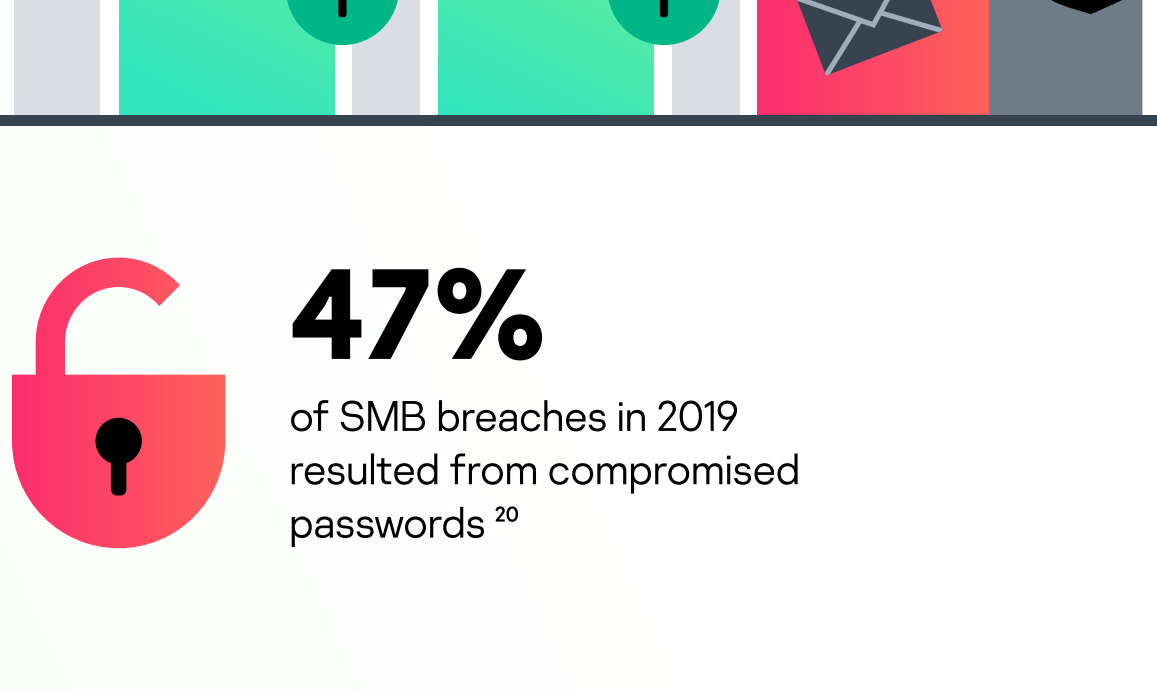
Password compromise in numbers

62% of SMBs allow reusing the same password on internal systems¹⁶

58% of SMBs have no control over employees' password practices¹⁶

68% of SMBs use weak passwords and deal with passwords being stolen or compromised¹⁶

¹⁶ Ponemon 2019 State of Cybersecurity in Small & Medium Size Businesses



47% of SMB breaches in 2019 resulted from compromised passwords¹⁶

What you can... and should do!

- 1 Install a Password Manager – one password to protect all.
- 2 Implement two factor authentication across your business.
- 3 At a minimum create strong passwords and change them regularly.

Conclusion

Promote awareness. Your best defense against malware!

Protect your small business with trusted cybersecurity. Learn more about Kaspersky Small Office Security.

[Learn more](#)

