Small Business Protection

Security guide

small businesses and freelancers

panda

Small Business Protection

We could give you a lot of reasons to elaborate this guide, but we think that one should be enough: 91% of small businesses and freelancers suffer daily IT attacks.

Yes, every day nearly 100% of small businesses or freelancers suffer some type of cyberattack that compromises the security of their businesses, data, and income.

Do you still think that it isn't necessary to protect your business on the Internet?

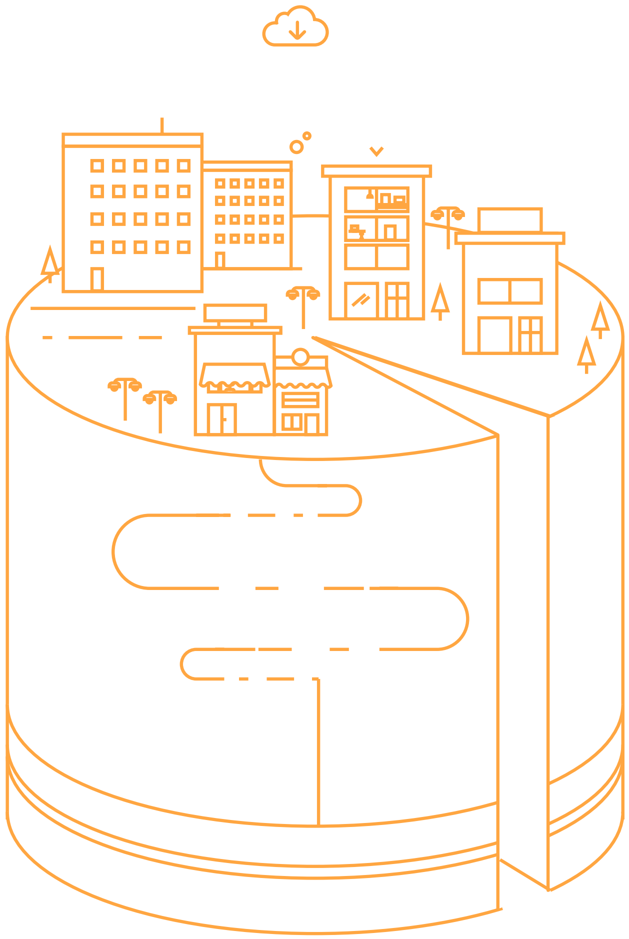
Take a look and we are sure that you will change your mind...

/91% of small businesses and freelancers suffer daily IT attacks

/ Every day nearly

100%

of small businesses and freelancers suffer some type of cyberattack



1

—

Where is the danger and how can we protect ourselves?

Social engineering

Cybercriminals can try to attack our businesses in two ways:

They pretend to be a representative from a reputed organization (the bank, the email provider, etc.) and, after various questions and warnings, ask for the access codes, having won the victim's trust.

Telephone

Internet

The most common method of fraud is called phishing*. The victim gives their data because they think that they are using a trusted website.

Another form of attack is by sending attached files in emails of known persons. The malware attacks the address book of the victim, sending each person an email which contains an attached file filled with malware.

How can we protect ourselves?

Train employees

The best way to prevent it is to try and educate our employees to be aware of social engineering tactics. See Do's and Don'ts

> See Do's and Don'ts of Cybersecurity

Be paranoid

It's recommended that we "cultivate a healthy paranoia", because it is common for cybercriminals to give up if they think the victim doesn't trust them.

Question everything

We should always ask the person that we're dealing with why they need the information. The majority of social engineering attacks fail when questions are asked.

Verify sources

If we are suspicious about a request that isn't usually made by email, then we should verify it by telephone. If we talk face-to-face with someone that we don't know, we should demand some type of personal identification.

Say no

When a cybercriminal is applying social engineering, it is usually done by departing from the norms of the business or making the victim do it. Keeping in line with company policy is your best defense.

*(see the description of threats in section 3)

Email

How can we protect ourselves?

A lot of the cyberattacks on businesses originate in emails that already have an important piece of information on the business.

Just like with social engineering, the first thing to do is train employees on IT security so as to avoid risky behavior when using corporate email.

Encrypt your emails. So that the company can control confidential information and that it doesn't pass through personal accounts, the best way to do this is to encrypt emails.

Delete old emails. If you have thousands of emails that you consider to be important, the best thing to do is save them on an external hard disk, on a database, or on the cloud. You can then eliminate them from your email account.

When you have to create a password, make sure that it is complex and that nobody can guess it, although keep in mind that you should be able to recall it easily if using it frequently.

Be careful when logging in from public computers. Make sure to end the session before leaving the computer as you might leave an easy trace for cybercriminals. It's best to access corporate information when you are using a trusted computer.

Don't give your address to everyone, nor should you leave it on public websites. Scammers are always waiting to pounce on any opportunity.

Take care with emails which try to trick you into creating a new password for better security. If you need to change your password, go to the website of the email provider and do it there, not on the link that comes in the email.

Continuing on from the point above; don't open emails that come from unknown or suspicious sources.

Don't forget to only use the corporate email as a work tool. It should never be used for personal reasons.

Teleworking

It without a doubt offers more flexibility to workers and makes them more productive.

But what about the security of it?

If employees are working from home, companies don't have the same protection and information loss can occur. Working from home invites a lot more risk, as the software available in the corporate environment usually offers better security guarantees.

The risks are varied and the loss of data can happen in different ways: an error on the computer that deletes files that don't have security copies, the theft of a password, or even a computer could lead to confidential data ending up in a cybercriminal's hands.

However, teleworking doesn't have to be dangerous.

How can we protect ourselves?

It's essential that there is a protocol in place that establishes how to act when working remotely in terms of security.

The use or remote desktops is a solution: with them it is possible to avoid information loss because it allows the employee to directly connect to the company's server, where all the information and security copies are automatically stored.

Another important point is about passwords. The theft of an employee's password could be disastrous, as it would put a lot of information at risk. It is important not to repeat passwords, change them every so often, and use a password manager to protect them.

It's also important to encrypt confidential information. This means that losing a laptop, or having it stolen, doesn't mean that the information is gone, too. Encrypting files via the operating system or encrypting the entire hard disk eliminates the risk.

One way or another, teleworking is growing at a fast rate thanks to technology, but it doesn't mean that security should be compromised. The right technology offers the tools so that information isn't at risk while employees work from home.

Cloud

Its ease of use has made us become more and more connected.

However, when using virtual storage to store and share information about your business, it's possible that its security measures leave a lot to be desired.

How can we protect ourselves?

Create secure passwords. You already know this... letters, numbers, upper-case, lower-case, symbols and, if possible, different passwords for different accounts.

As regards the encryption of files, some of the virtual storage services keep our documents encrypted.

Dropbox doesn't do it, but Mega does. However, none of them are perfect: mega keeps a copy of the code to decrypt them on its servers, which doesn't seem to be 100% secure. A good option is that you be the one to encrypt them before storing them on the cloud.

Dropbox and Google Drive allow the activation of the two-step verification process. This system combines the password that you use with another that is sent to your mobile device (nearly always a mobile phone and via an SMS or app), ensuring a second security layer.

Mobile devices

A company isn't secure if it is only protecting the traditional limits. Now it is essential to have a strategy in place for corporate mobile devices, one which, apart from guaranteeing their security, also incorporates the protection of information and the applications use don them.

According to a report by Nielson for Panda Security on the State of Protection for small businesses and freelancers, 25% of corporate tablets don't have security software. This figure rises to 35% for smartphones. These are figures which show why a lot of current attacks are targeted at mobile devices.

In addition to protection, the mobile security strategy has another requirement: not to hinder business agility and dynamism that the use of mobile devices provides

How can we protect ourselves?

One of the first things is to install security software on mobile devices. In recent time we have seen the operating system (especially Android) become a target for cybercriminals.

The user identification needs to be more robust than just a traditional password. Many mobile devices allow us to use our fingerprints as identification and companies should train their staff to use these tools as well as what to do if they lose the device or it is stolen.

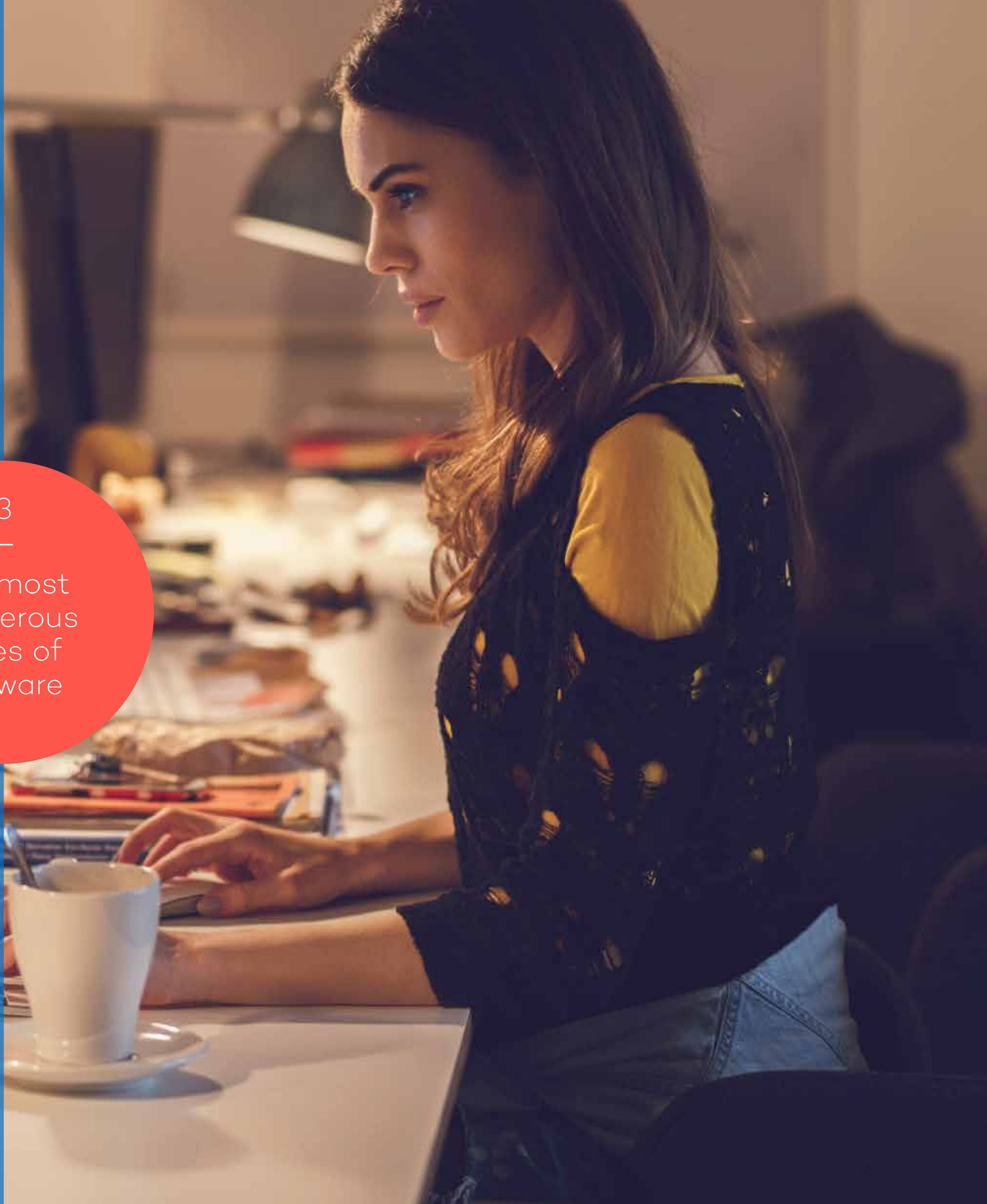
Be careful with third-party software: many professionals install apps from suspicious sources which, despite appearing trustworthy, turns out to be an imitation page created by cybercriminals.

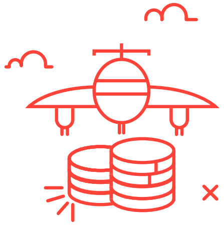
Just like before, mobile devices need to be set up to avoid wireless networks that aren't secure and recommend to users that they disable the Bluetooth option to avoid any surprises.

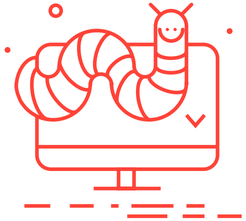
3

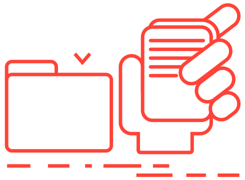
—

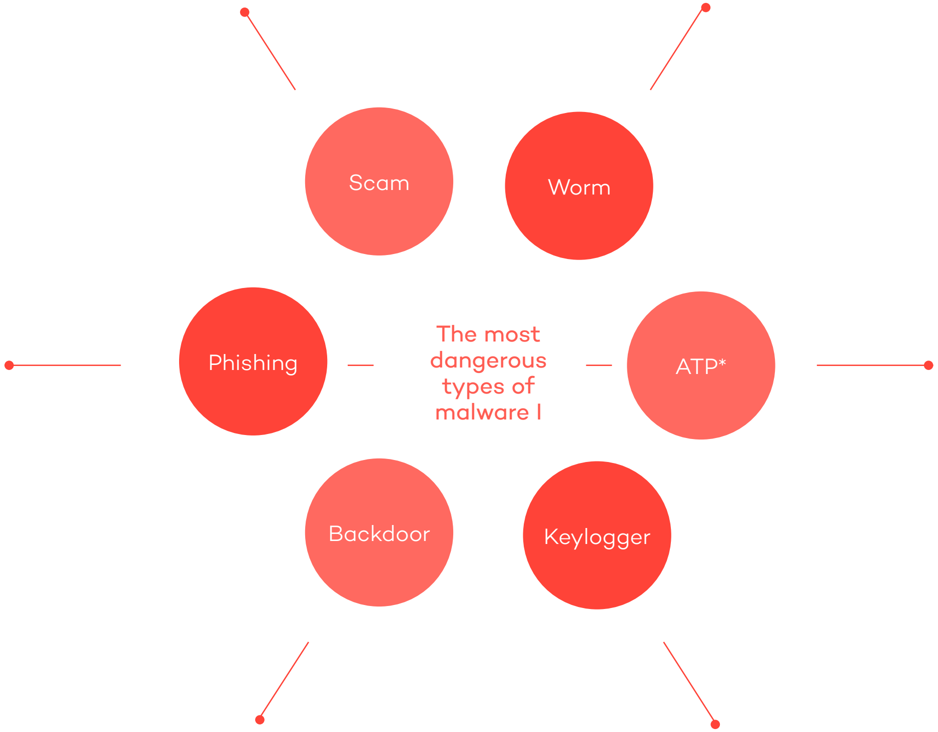
The most dangerous types of malware











The most dangerous types of malware I

Scam

It tricks you with promotions for holidays and lotteries, and asks for money to access the supposed prize

Worm

It infects the computers connected to the network and even blocks access to communications.

Phishing

It creates a false URL to obtain your information and to steal your identity, thus being able to rob from your bank accounts.

ATP*

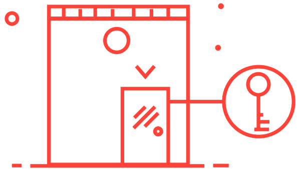
It breaches your security so as to control and monitor it, being able to then extract information continuously.

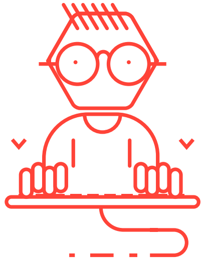
Backdoor

It opens a back door and takes control of the affected system.

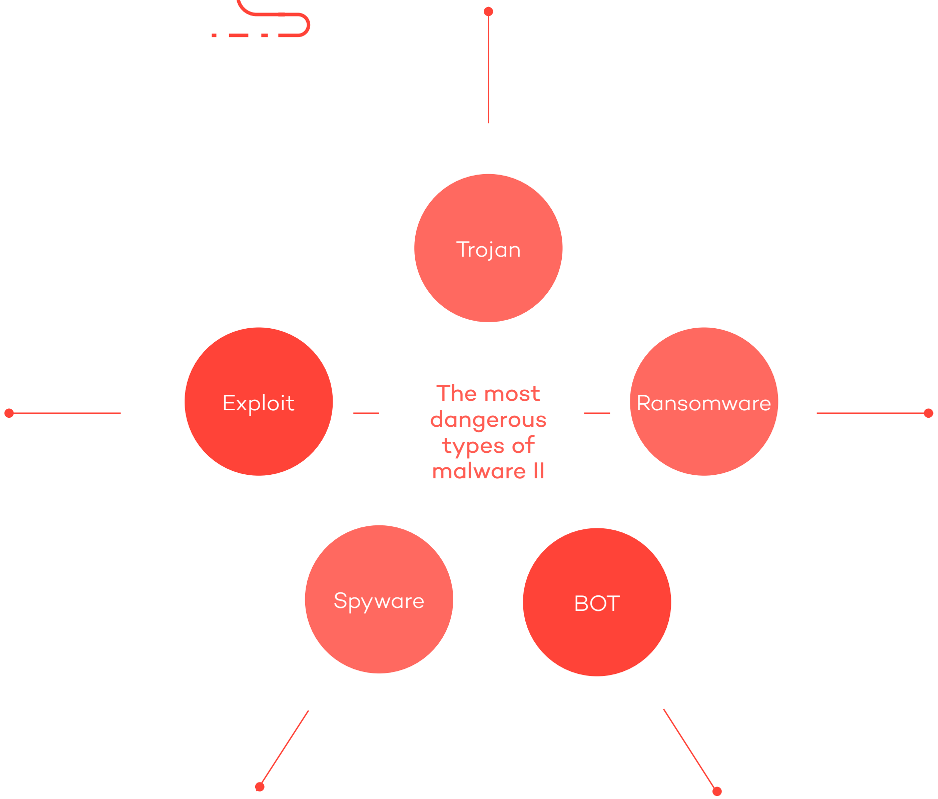
Keylogger

It collects, saves, and sends all of the inputs on the keyboard.





* Advanced persistent threat



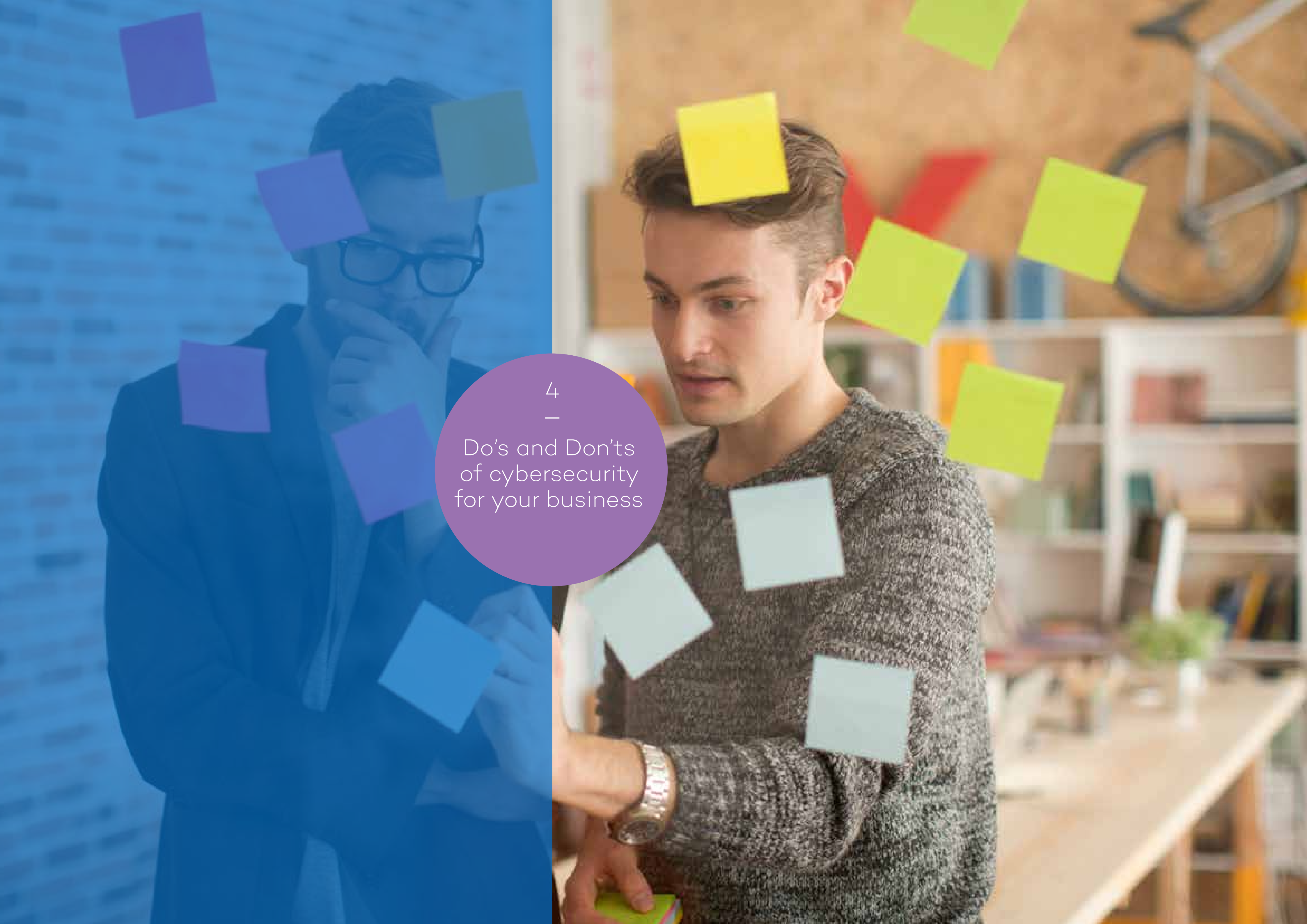
It installs various applications so that hackers can control your computer, your files, and steal confidential information.

It blocks the PC, takes control, encrypts your files, and demands a ransom to return them to you.

It is a program which, once inside your computer, allows us to control it remotely

It collects names, accounts, access codes, and any other type of information on the organization

It takes advantage of a security flaw in communication protocols to enter your computers.



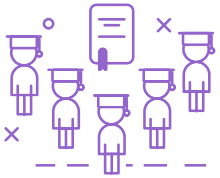
4

—

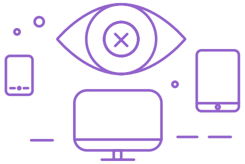
Do’s and Don’ts of cybersecurity for your business

Do's and Don'ts of cybersecurity

1 Train your employees
Their security knowledge will save your company from a lot of problems.

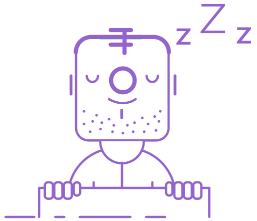


2 Pay attention to mobiles and tablets, not just computers.

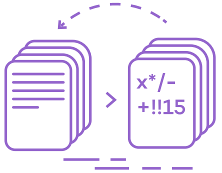


3 Be careful with links that you receive in your corporate email. If suspicious don't open them.

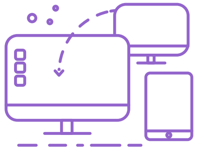
4 Use a security solution that allows you to sleep easily.



5 Encrypt your most valuable information.



6 Use remote desktops for teleworking

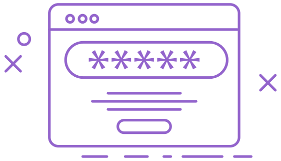


7 Avoid installing suspicious content from third-parties in your business

8 Make security copies of important information.

9 Be careful using when using a corporate device.

10 Create complex passwords using different cases and symbols.



/Will you let us protect you?

After all of this information and advice that we have given you to help ensure that your company is protected against cyber-threats, the next step is to give you a solution that will protect you from threats while online.

Small Business Protection

Our antivirus for small businesses and freelancers, Small Business Protection, won't just help you to eliminate viruses and all types of threats on your devices, but it is also especially designed so that you don't have to worry about a thing. Its installation is easy and it doesn't need any maintenance.

Simple, right?

Discover more

The protection you need with the best value for money

Lightweight, powerful antivirus suited for new and older PCs

Download it and get protected without any technical assistance

Small Business Protection

Panda Mobile Security

Also, for your Android devices, there is nothing better than Panda Mobile Security. This solution will give you peace of mind at all times when it comes to your Android mobile phones and tablets.

Discover more

Panda Antivirus for Mac

Finally, if you are a Mac user, we're sure that after reading all of this you aren't one of those who thinks Apple is immune to viruses. That's why we offer you Panda Antivirus for Mac, which allows you to block malware for Mac, iPhone, iPad, and even iPod Touch.

Discover more

So now you have no excuse,
why wait any longer to protect your business?

panda