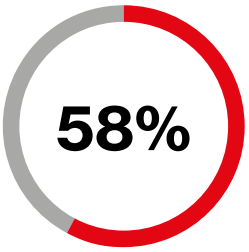
# Don’t ignore cybersecurity: Avoid these 3 common excuses.

Point of view

**To cybercriminals, your customer records, personal information and payment card data are all just another opportunity to make money. And the techniques they are using to turn your precious data into cash in their pockets are getting more and more sophisticated. But many businesses still take a dangerously relaxed attitude to cybersecurity. Are you guilty of using one of these common “reasons” not to do more about the risks?**




Nearly three-fifths of the victims in this year’s Data Breach Investigations Report were categorized as small businesses.

## Complacency – it’ll never happen to me

You’re more likely to be struck by lightning than suffer a cyberattack, aren’t you? It’s other people that get hacked, big companies and banks, right? Wrong on both counts. Small businesses are actually a big target for criminals. The 2018 edition of our annual Data Breach Investigations Report found that well over half (58%) of the victims fell into the small business category.

Fortunately, there are simple steps you can take to protect yourself from three of the most common types of incident.

**Don’t get caught by phishing**
Many people still fall for scams where cybercriminals trick you into clicking on a malicious link or email attachment. It only takes one victim for your systems to become infected. Train your employees to spot the signs of a suspicious email or document. And if your email system offers the option to flag emails from an unknown contact – most leading ones do – turn it on. Then the recipient will know to proceed with extra caution.

**Protect against ransomware**
This is when cyberattackers block access to your data or systems and demand a ransom to let you back in. Don’t give in to them – paying up is no guarantee that your systems will be restored. Protect your business and back up your data to the cloud. So even if a hacker does encrypt your files, you can get back up and running.

**Reduce human error**
One in six (17%) of the breaches examined in this year’s Data Breach Investigations Report were caused by a slip up. We all make mistakes, but there are ways to reduce the risk. Teach your employees not to leave their devices unattended, and to securely dispose of confidential information – whether it’s physical or virtual.

verizon business ready

## Cost control – I can't afford better cybersecurity

A strong defense doesn't have to cost a fortune. There are simple and cost-effective steps you can take to protect your business from cybercrime. These are some things you can do that won't break the bank.

**Install updates promptly**
Always install updates promptly. Not just on your computers, but tablets, POS systems and your website too. Cybercriminals are still making use of vulnerabilities from months or even years ago – don't put your customers' data at risk because of something you could have easily avoided.

**Secure all your devices**
Whether it's a laptop, a smart thermostat or a smart speaker, if using a password – or PIN or other security option – is an option, turn it on. And never, ever, rely on the default password that it comes with – those are easy to find online. A device management solution can help keep your devices secure.

**Limit access of personal devices**
Don't let employees connect their personal devices to your business network. You have no control over what risks they take, and they could inadvertently infect your systems. Instead, use your router to create a guest Wi-Fi network for employees. Plus, with some networks you can connect multiple devices and users at the same time, so you don't have to worry about overloading the system.

**Have an incident response plan**
Create a response plan. Define clear processes and make sure your employees know what to do if they spot anything suspicious. And test it, a real incident is a really bad time to find what you missed out.

**Block harmful traffic**
For extra peace of mind, get Verizon's DNS Safeguard to help stop threats before they start. It's a cloud-based security platform that provides a first line of defense against internet-based threats. It automatically blocks your computers and other devices from accessing malicious sites and content.

## Procrastination – I'll sort that next week

Cybersecurity can seem daunting, and it's tempting to put it off. But that can be a dangerous gamble. Start overcoming the inertia by taking some of these quick and easy to implement steps.

**Train your employees**
Teach your employees how to spot the signs of a cyberattack and what steps to take if they do. Early detection can help mitigate the attack and limit the damage. This can be as simple as holding an afternoon training session – ongoing reminders help too.

**Back up your data**
It doesn't have to be tedious or time-consuming, and could save your bacon. Take advantage of available cloud services to securely back up and store your data.

**Invest in a tailored solution**
Invest in a cybersecurity solution specifically designed for small businesses like yours. Verizon's packages help to safeguard your devices from viruses, spyware, phishing and more – all for a simple monthly fee.

## Get the help you need to improve your defenses

Effective cybersecurity doesn't have to be complicated or expensive. Verizon understands the challenges your business faces and has a range of products built with you in mind, no matter your size. Take action on your cybersecurity and give your business the defense it deserves.

**Find out more** >

verizon business ready