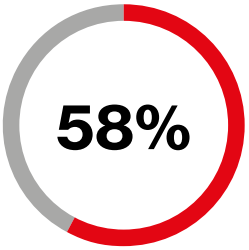
Cybersecurity: Are you making these 3 common mistakes?

Point of view

Protecting your business from the ever-changing mix of cyber threats isn't easy. It can be even more difficult for smaller businesses, which often don't have the expert knowledge or resources required to outsmart the criminals.



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

But with 58% of the data breach victims in this year's Data Breach Investigations Report categorized as small businesses, knowing how to strengthen your defenses is vital. Protecting your business needn't be complicated or costly.

Here are some common ways companies put themselves at risk and ideas for avoiding them.

Cutting corners

Nobody likes passwords. It seems like we need more each year and the temptation to use, and even reuse, ones that are easy to remember is high. The solution to this problem seems straightforward, but it can be hard to change people's habits. There are things you can do.

Use two-factor authentication
Many of the web apps small businesses rely on – like Microsoft Office 365, Google Cloud G Suite, Sage and Xero – offer two-factor authentication. Use it.

Change default passwords
Change the default passwords on every new device your business buys: routers, wireless access points and Internet of Things (IoT) devices – like smart thermostats or security systems.

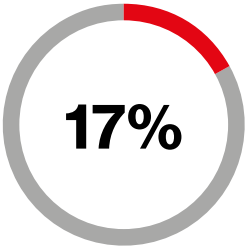
Manage your passwords
Use a password manager app – like Dashlane – to make it easier to use complex, strong passwords and give you early warning of potential compromises.

Be wary of public Wi-Fi
Remember that there's no such thing as a free lunch. You want to have access to your email and business apps when you're out of the office, but there are dangers with relying on public Wi-Fi – take a look at our Mobile Security Index to find out more. Our 4G LTE network offers a reliable way to stay connected, and we offer a range of compelling plans to cover all your devices.

verizon business ready

Being human

We get it, mistakes happen. But they can have a bigger impact on your business than you realize. Errors were at the heart of one in six (17%) of the breaches covered in this year's Data Breach Investigations Report – including employees failing to shred confidential information, sending emails to the wrong person and misconfiguring web servers. Assuming replacing your staff with robots isn't an option, how can you help prevent these mistakes?



Errors were at the heart of one in six of the breaches covered in this year's Data Breach Investigations Report.

Check before you hit send
Teach your staff to perform appropriate checks, like checking the recipients on an email chain and enforce strict policies on using mobile devices and social media. Some web email services can provide warnings when you're sending a message to somebody not in your contact list. Switch it on.

Have an incident response plan
Introduce procedures for dealing with incidents – it can be as simple as making sure everybody knows who to contact, even out of hours. This can help you mitigate the damage should mistakes happen.

Block harmful traffic
Even with the best training, your staff will still be fallible – we all are. Services like Verizon's DNS Safeguard can help you put measures in place to block harmful web traffic and shield your network from internet threats like malware and ransomware; doing so can reduce the likelihood of employees accidentally clicking on malignant websites and causing an incident.

Limit access
Set access controls so employees only have access to devices and data on a "need to know" basis. By limiting access to only what they need to do their job, you can reduce the risk of employees sharing data, misusing it, or exposing it – whether intentionally or by mistake.

Taking the bait

Phishing remains one of the most common tactics cybercriminals employ. It usually involves sending an email with a malicious link. Many of the bad guys are very good at enticing people to click. And they do. This year's Data Breach Investigations Report found that four out of five (78%) people didn't click on a single phishing email all year – but that means that 22% did. Attackers are also finding new ways to make crime pay. Ransomware, where a hacker locks your data and demands money from you to get it back, is now the most common form of malware.

Train your employees
Train your employees to identify suspicious emails and make it easy for them to report any they find. Our analysis found that only one in six (17%) phishing campaigns were reported; by having a policy in place you can help reduce the likelihood of falling victim and contain any damage caused if you do.

Back up your data
Back up your data – whatever device it lives on. As well as being good for disaster recovery, it can massively reduce the impact of a ransomware infection. The easiest thing to do is to regularly back up your data to the cloud. This keeps your data secure and means it's available when you need it.

Flag external emails
Set up your email system to flag emails from external sources. Perpetrators have swindled businesses out of millions of dollars by posing as a colleague and duping somebody into making a fraudulent payment – it's called financial pretexting. Reduce the thieves' chances with this really simple and cheap technique.

Get the tools you need

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. Avoid making the usual mistakes and give your business the protection it deserves. To learn more, contact your Verizon account representative or have us contact you.

verizon.com/business

verizon business ready