

SCANNING...



How to protect your business online



A complete guide to shielding
your company from 3 major risks



Contents

00 - Introduction	3
01 - Protect your brand and reputation as your digital footprint grows	4
Reputation is a priceless asset	5
Design a domain name strategy	6
Safeguard your brand through domain security	7
Maintain brand trust with business continuity	8
02 - Build financial stability to withstand unpredictable markets	10
Cash is king	11
Account for digital infrastructure in your financial planning	12
Choose a hosting provider with granular subscription types	13
Acquire easy-to-use security tools	14
03 - Defend against cyberthreats	15
Take charge of your security	16
Follow cybersecurity best practices	17
Prioritise security for DDoS attacks, a rising cyberthreat	19
Enhance your email security	20
Build a secure future for your business	21

Introduction

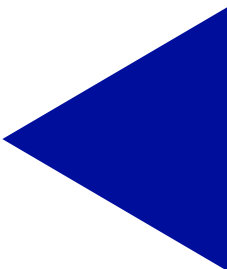
BUSINESS GROWTH COMES WITH MORE OPPORTUNITIES — AND RISKS

As the digital landscape rapidly expands and evolves, so do the risks that small and midsize businesses (SMBs) face.

You know you need to enhance your online presence to succeed in today's competitive market. To fully reap the benefits of digitisation — such as scalability, greater productivity, improved customer experience, and exposure to a global audience — it's essential that you develop a plan to build a strong digital infrastructure.

There are three major risk types — reputational, financial, and cybersecurity — that you must be prepared to address while growing online. Fortunately, doing this is less complex than ever before. Vital solutions for protecting your business (e.g., web hosting, domain security, data backups) have advanced to a point where you no longer have to hire full-time technical experts or work with several costly vendors to achieve your goals.

Here's how you can take practical actions and embrace user-friendly technology aiming to protect your business and stand out from the competition with a winning digital strategy.

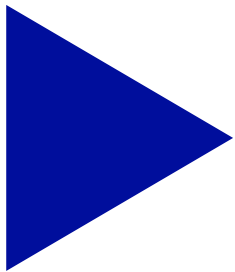




01

**Protect your
brand and
reputation as
your digital
footprint grows**

Reputation is a priceless asset



90% of online shoppers have chosen not to purchase from a company because of its bad reputation.¹

Brand and reputation management become increasingly important as your business scales its digital footprint. Expanding to multiple online platforms — such as your website, social media, and email marketing — means that you can interact with more potential customers. A bigger audience, in turn, opens up additional opportunities for sales and growth.

A trustworthy brand reputation not only helps attract new business, it also helps maintain loyalty among current customers. Research from Trustpilot¹ found that “good online reputation” is the number one factor that increases trust. More than 95% of consumers believe that reputation makes a tangible difference in their willingness to buy from a brand.

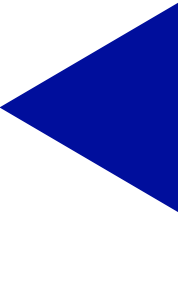
However, this is a two-way street — as your online presence grows, the thoughts and opinions of your customers are also amplified via social posts, blogs, reviews, and more. A single bad experience can be broadcast to a large audience, damaging your reputation and prompting buyers to look elsewhere.

Here are three steps you should take to help your brand uphold an excellent reputation so that it is perceived as trustworthy online.

¹ [TrustPilot, The Value of a Trustworthy Brand Reputation Report](#)

DESIGN A DOMAIN NAME STRATEGY

Choosing and preserving the right website domain name is crucial to making a good first impression. A domain name is a unique address that is used to access your website (e.g., ovhcloud.com). But it is much more than just a web address — a domain name is part of your company's identity.



A strong domain name should be short, memorable, and relevant to your brand.

When acquiring a domain, you must design a strategy to protect your business from reputational risk. Domain fraud, for instance, is a common tactic that bad actors use to impersonate a brand and trick users into divulging sensitive information. For example, cybercriminals might try to register domain names that are similar to yours and contain a domain extension that is slightly different (e.g., .co instead of .com) or a misleading extension that is related to the purpose of your website (e.g., ovh.cloud instead of ovhcloud.com).

To mitigate reputational risk that comes from domain fraud, you should register domain names that will minimise such threats. OVHcloud makes this easy by [automatically suggesting options](#) from our catalogue of more than [900 extensions](#) that are widely used in the market (e.g., .com, .net, .org), relevant to your location (e.g., .fr, .eu, .uk), and related to your industry (e.g., .fashion, .health, .tech). You can even use OVHcloud to register common misspellings of your domain or names that look visually similar (e.g., a 0 in place of an o).

It's also critical that you maintain ownership of your domain names for as long as possible. Loss of a domain name can lead to reputational damage (customers are confused when they land on a different website) or even exorbitant costs to get the name back from [cybersquatters](#) who exploit this mistake for their own gain. For this reason, OVHcloud automatically renews domain names by default so you reduce the risk that someone else will take your name.

Safeguard your brand through domain security

In addition to a strong domain name strategy, there are other measures you should take to shield your domain from cyber risk. Bad actors may attempt to employ techniques such as domain slamming (i.e., illegitimate transfer requests) and [cache poisoning](#) to redirect users to another website, which they could use for phishing attacks, distributing spam, or hosting malicious content. This can severely damage your reputation and erode trust with customers.



We suggest that you follow all of these steps and adopt a multilayered approach to domain security. This way, if a cyberthreat bypasses one type of security measure, there is another layer in place that is designed to stop that type of attack.

To defend against these sophisticated types of domain attacks, OVHcloud offers a simple, “push button” approach that allows you to easily:

► 1

Activate [Domain Name System Security Extensions \(DNSSEC\)](#) to protect against cache poisoning, a cybercriminal tactic used to divert traffic to malicious websites.

► 2

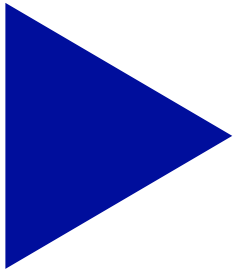
Trigger a mechanism to [prevent your domain from fake renewal notices and other fraudulent transfer requests.](#)

► 3

Adopt website and email security mechanisms, such as Secure Sockets Layer (SSL) and Transport Layer Security (TLS) certificates.

Maintain brand trust with business continuity

Of course, it's impossible to eliminate digital risk with 100% certainty. That's why you need to have a plan ready in case something (e.g., a cyberattack or traffic spike) threatens to take your website offline. Website downtime can frustrate customers, hurt revenue, and cause long-lasting reputational damage.



Downtime can cost small businesses up to \$427 per minute.²

A digital continuity plan helps you remain prepared to keep your website running with little to no downtime in the event of an incident. It is an integral part of your reputation protection strategy that keeps your online presence stable. A continuity plan should include steps such as:

- Identify your most valuable applications and data that are required for business continuity.

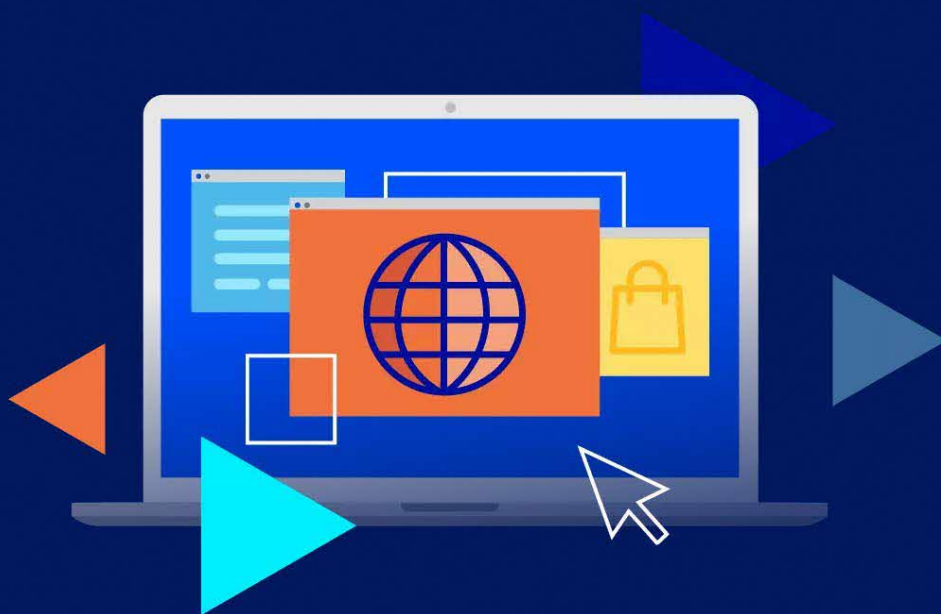
- Ensure that only trained employees with sufficient IT expertise have access to modify critical services that could put the system down.

- Routinely [back up critical data and systems](#) (e.g., files, content, databases, etc.) so your website can be restored quickly if needed.

- Choose a reputable provider that can provide [optimal uptime](#) for your website's essential functions while providing options for disaster recovery if needed.

For web hosting customers, OVHcloud monitors the network to detect hacking attempts, such as an abnormal amount of queries on the server, and issues an alert so you can take immediate action to resolve the problem.

² [Pingdom, Average Cost of Downtime Per Industry](#)



OVHcloud web hosting also includes automatic backups to preserve data integrity and support quick recovery (e.g., if you make a mistake managing your website), allowing your business to minimise downtime and maintain a positive reputation. We also suggest that customers perform a “3, 2, 1” backup strategy:

▶ 3

Create **three** copies of your data (i.e., the original, plus two backup copies).

▶ 2

Store them on **two** different mediums (e.g., disk on a remote site, cloud storage, etc.).

▶ 1

Keep **one** copy offline on a storage solution disconnected from the rest of the network, or on one removable storage medium.

Working with multiple vendors to acquire the technology needed to follow these best practices can be expensive and difficult to manage. OVHcloud, on the other hand, is a single, cost-effective website partner that provides tools contributing to keep your domain and reputation safe.

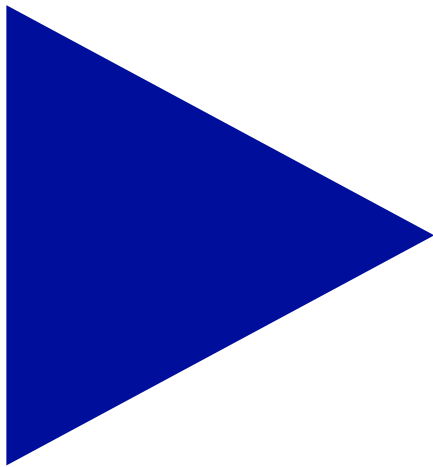
02

**Build financial
stability to
withstand
unpredictable
markets**



CASH IS KING

Cash has become a key asset for every company, no matter the size. But SMBs, in particular, are still recovering from the devastating financial effects of the pandemic, which means they often have limited cash flow and very little tolerance for unexpected costs.



“Never take your eyes off the cash flow because it’s the lifeblood of business.” – Sir Richard Branson

It’s important to achieve stability and predictability with your cash position. However, you may be disheartened to learn that many of the products and services you are considering to build up your online presence come with overage charges, renewal fees, and other hidden costs. They might also lock you into a long-term relationship.

For example, some web hosting solutions initially seem attractive because they are user-friendly (due to limited customization). However, down the line, these seemingly low-cost solutions can become prohibitively expensive, as you’d have to start all over again if switching to another provider.

Here are three steps you should take to keep your business from taking on too much financial risk in launching and maintaining your website.

ACCOUNT FOR DIGITAL INFRASTRUCTURE IN YOUR FINANCIAL PLANNING

Online expansion should ultimately boost, not hinder, your business's profitability. If this is your first time investing in one or more of these digital capabilities, it's crucial that you plan ahead and ask the right questions to control costs, avoid financial strain, and support long-term scalability.

Key steps to consider in the financial planning around your online infrastructure include:

Assess current expenses:

Review your digital costs (e.g., software licences, social media tools, email services, etc.) and confirm that every expense is delivering value in terms of revenue, time savings, brand equity, or customer satisfaction.

Budget for additional services:

Knowing that your website naturally comes with hosting and security requirements, carve out a section of your monthly/yearly budget to allocate toward these services.

Define hosting needs:

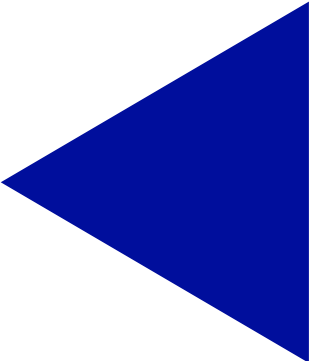
Compare hosting providers based on factors like pricing, features, customer support, and optimal uptime, prioritising those that have [transparent pricing and no surprise costs](#).

Look out for lock-in:

Some companies make it very difficult to switch providers and infrastructure without extremely high costs. To avoid this, ask questions such as, "Do you offer full reversibility?" and "How do you prevent vendor lock-in?"

Consider scalability:

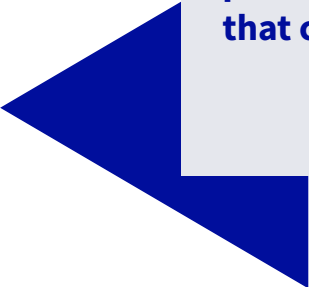
Choose a provider that enables scalability — both vertically (e.g., [hosting upgrades](#)) and horizontally (e.g., [additional services](#)) so that your hosting plan can grow with your business's needs.



OVHcloud aims to make your financial planning as easy as possible with pricing transparency. We also offer [virtual private servers \(VPS\)](#) and [dedicated servers](#) if you ever decide you need greater control over your servers to build web applications, more complex websites, and digital infrastructure.

CHOOSE A HOSTING PROVIDER WITH GRANULAR SUBSCRIPTION TYPES

It's important to partner with a web hosting provider that allows you to fine-tune a subscription that includes only the features and benefits that will be valuable to you. You want to pay for only the features and services you will use, with the ability to modify your subscription as your business needs change.



Would you rather choose from a small, rigid selection of plans or a full spectrum of flexible subscription options that can be tailored to your needs?

OVHcloud offers subscription options, which means you are getting the ideal price for the features and functionality required for your website. We always aim to offer the ideal price-to-performance ratio for all of our services.

With OVHcloud, you know exactly what these costs will look like each month, which makes financial predictability and forecasting less stressful. We know the one-size-fits-all policy is not what you are looking for. This is why we build granular price plans to propose what you really need at each stage of your project.

Acquire easy-to-use security tools

SMB security is an often-overlooked aspect of financial stability. A strong website aims to protect sensitive data, maintains customer trust, and mitigates financial losses that can result from a breach or fraudulent activity. This is a growing threat in today's digital landscape — global research from Mastercard³ indicates that European businesses face high fraud risk.

Two out of every
three online retailers
in Germany have
noticed an increase
in online fraud.³

If you handle or process financial information we suggest using trusted, up-to-date tools and plugins (e.g., PayPal, Stripe, etc.) that can easily integrate with your content management system (CMS). Both CMS and payment processing companies frequently update their software based on evolving threats, so it's important to update your tools and plugins regularly.

With OVHcloud, you can rest assured that we will shield your website hosting infrastructure so you can focus on identifying critical or sensitive data and developing a plan to protect this information.

³ [Mastercard, Ecommerce Fraud Trends and Statistics Merchants Need To Know in 2023](#)

03

Defend against cyberthreats




Take charge of your security

Cybercriminals don't always choose targets based on business size or type. Instead, they look for easy openings, such as an outdated CMS or weak security policy, to exploit. In addition to data theft, bad actors can use a breach to manipulate your services and brand or to impersonate your business to help them carry out future attacks.

Taking steps to mitigate security risk is now a business requirement. But many organisations don't feel prepared to deal with today's cyberthreats. In a survey of small- and medium-sized enterprises (SMEs) across the EU⁴, 90% said that cybersecurity issues would have a serious negative impact within a week of an incident occurring.

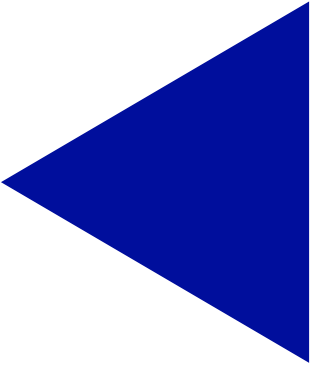
Over half (57%)
of SMEs believe
they would most likely
become bankrupt
or go out of business
after a cybersecurity
incident.³



While cybersecurity may seem daunting, there are many simple yet impactful measures you can implement to significantly reduce risk. Here are three steps you should take to improve the security posture and resiliency of your business.

⁴ [European Union Agency for Cybersecurity, SME Cybersecurity Report](#)

FOLLOW CYBERSECURITY BEST PRACTICES



Cybercriminals often use automated tools to scan thousands or even millions of business entities to identify attack vectors to exploit. It's in their interest to find something they can quickly take advantage of with minimal effort. In fact, research⁵ shows that the most common vectors include stolen credentials (i.e., username and passwords), phishing (i.e., sending fraudulent emails on your behalf), and vulnerability exploitation (i.e., a bug or flaw in a system).

It's vital that you and your employees all take proper precautions to mitigate the risk of these attacks damaging your business. According to a report from the World Economic Forum⁶, 95% of all cybersecurity issues can be traced to human error. Thankfully, you don't have to start from scratch to reduce your cyber risk, as there are established, time-tested best practices you can use to protect your business. These include:

Implement strong password policies:

Enforce the use of complex passwords and [multi-factor authentication](#) to block low-level attempts to bypass security.

Conduct regular updates and patching:

Keep all software, including operating systems, applications, and plugins, up to date and patch known vulnerabilities.

Encrypt your data:

Use encryption protocols to provide security for data in transit and to encrypt sensitive information stored on servers and in databases.

Install firewalls:

Implement firewalls to monitor and filter network traffic, helping to prevent unauthorised access and detect suspicious activity.

Perform regular data backups:

Back up critical data, confirming that information is stored securely and can be restored in the event of a cyber incident.

Understand your obligations:

Recognize the importance of shared responsibility and [what you are expected to do](#) (e.g., conducting regular software updates) with the tools you are provided.

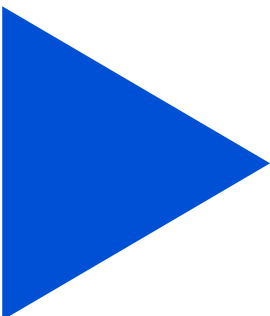
⁵ [Verizon, 2023 Data Breach Investigations Report](#)

⁶ [World Economic Forum, Global Risks Report 2022](#)



There is no perfect, one-size-fits-all solution for complete security — a layered defence is the only viable defence.

At OVHcloud, we offer packaged security solutions for your digital journey. For example, all of our domain services include [DNSSEC](#) for managed security of your domain name, and our web hosting services include [SSL certificates](#) for data encryption.





Prioritise security for DDoS attacks, a rising cyberthreat

Distributed denial-of-service (DDoS) attacks, a malicious tactic for obstructing service to a website, are becoming more prevalent and more frequent. The barrier to entry here is very low — almost anyone can carry out a DDoS attack with a cheap set of automated tools.

These attacks are unique in that they typically don't involve a security breach or data theft. The goal is simply to take down your website. Perpetrators could be criminals trying to request a ransom to restore services, malicious competitors who want to tarnish your reputation, or simply digital vandals looking to cause trouble.

DDoS attacks are up 200% year-over-year.⁷

That's why you should confirm that DDoS prevention is included in your website to protect against this common threat. While this can be difficult to carry out on your own, the good news is that OVHcloud hosting services come with security mechanisms, including [anti-DDoS](#). This includes:

Always-on attack detection and rapid mitigation of malicious traffic.

Unmetered usage, which means no additional cost regardless of attack volume.

No time limit, with protection lasting the full duration of a DDoS attack.

Our anti-DDoS technology runs seamlessly in the background of your website. No matter how many times hackers attempt to overwhelm your servers, OVHcloud will endeavour to deflect attempts so that your perception of any type of disruption is minimized.

⁷ [Zayo Group, The Truth and Trends of DDoS Attacks](#)

Enhance your email security

Business email compromise (BEC) is a very common type of attack in which criminals send fraudulent emails, often imitating those within a company, to steal sensitive information. When successful, these attacks can be difficult to detect because they often don't trigger security alerts. The fraudster may have access to critical information and/or systems for months at a time.

It takes an average of 266 days to identify and contain a data breach resulting from business email compromise.⁸



OVHcloud offers robust authentication, anti-spam mechanisms, [SPF, DKIM, and DMARC](#) protocols automatically installed, that significantly reduce your risk of an email-related incident. These email authentication methods protect your business from unwanted emails and spam, preventing data alteration such as email spoofing (i.e., forging a sender address). While many providers make customers set up these features on their own, we configure these security measures for maximum efficacy.

When choosing OVHcloud for your [email services](#), you can also take comfort in knowing that our solutions operate across three different data centres. This means your communications will continue to run smoothly even in the event of an outage or service disruption for one location.

⁸ [IBM Cost of a Data Breach Report](#)



BUILD A SECURE FUTURE FOR YOUR BUSINESS

Your brand and reputation, financial standing, and security posture are all deeply intertwined, which means you should not skip or ignore any of the above steps without risking the integrity of the entire business.

Fortunately, taking the necessary measures to protect your business is less stressful and more manageable than ever before. Instead of vetting and investing in many different, expensive point solutions, you can partner with OVHcloud, an affordable, one-stop shop for your digital needs

[Learn more about our domain and web hosting solutions](#) to see how we can support the success of your digital strategy.

