

Account Security

At Namecheap we believe all of our customers deserve the best in account security. To protect your account, we offer:

- ▶ **Custom security notifications** so you can choose the circumstances in which you will be notified when your account is accessed.
- ▶ **Custom password recovery** options so you can decide on your password reset process in advance.
- ▶ **Dynamic support pin numbers** to protect against unauthorized attempts to gain access to your account.

Customers can update account settings at any time using our [custom security panel](#).

Domain Lock

One of the most common ways hackers take over websites is by attacking the very core of what a website is: the domain name.

Our [Domain Lock](#) security comes free with every domain we sell. It prevents unauthorized transfers of your domain by anyone pretending to be you. It's automatically enabled on all domains, so you're protected by default.

DID YOU KNOW?
If your domain gets stolen, it can cause irreparable harm to your business. Using a registrar that protects your domain from unexpected and unauthorized transfers is the best way to combat this. Symptoms of a stolen domain can include:



Drop in Google ranking



Slow-down in your business or e-commerce



Email address failure



Inability to reset email passwords



Your domain being pointed to embarrassing or illegal content

Namecheap's Account and Website Security Features

You need peace of mind when it comes to security threats. That's why, at Namecheap, we go the extra mile to protect the security and privacy of all of our customers, with our top-notch domain and account security.



DDoS Protection

Another way people bring down websites is by using 'bots' to send thousands or millions of requests to their servers, causing them to exceed quotas or crash. This is called a DDoS attack. If you use shared hosting, your personal site could be affected even if it's another site on the server that is targeted.

All of our servers have protection against DDoS attacks, and our teams are on hand to help out if your server falls victim to a DDoS attack.

Two-factor Authentication (2FA)

Most Internet accounts use a username/email address plus a password to authenticate a user. For many people the username is easy to guess or figure out, so your account security is only as safe as your password. If your password gets compromised (brute-force attacks, poor password security, or even just a lucky guess) it's easy for a hacker—or an angry ex—to gain access to your accounts.

DID YOU KNOW?

2FA works by combining two different types of authentication:



Something you know (typically, your username and password)



Something you have (your mobile device)

Anyone trying to access your account illegally won't be able to get past the second authentication. We offer 3 types of 2FA, free with all Namecheap accounts.

U2F

With U2F (Universal 2nd factor) you don't need to type in codes from an app on your smartphone. Instead, this technology uses a small, specialized USB or NFC device like Yubikey that contains your encrypted information.

TOTP

TOTP stands for Time-Based One-Time Password. This is a standardized method for generating a regularly-changing password that is based on a shared secret, ensuring that each code is unique.

OneTouch (SMS)

Use OneTouch (SMS), or the updated Namecheap App to authorize logins securely from your phone, safe in the knowledge that only you can do this as it uses your phone number. This is one of the easiest ways to approve your login or password reset requests.

Learn More about Online Security

Check out our [Privacy Guide for Small Businesses](#) for more tips on how you keep your important accounts and websites secure.