Domain Name Basics Security and Privacy

Tobias Sattler
tobiassattler.com

Domain Name Security

Preventing unauthorized access to your domain registration account and your domain names is **essential** because no one wants to lose a domain or even worse your business.

This presentation takes a more in-depth look and highlights a few **essential tips** on securing your or your organization’s assets **against theft** and **loss**.

These tips are not intended to be exhaustive.

Risk Scenarios #1

You begin the day as an online shop provider on example.com. At noon your visitor traffic and merchant transactions disappear.

You investigate and discover someone used your company's administrative contact, transferred your domain name to a different registrar, and modified the DNS.

As a result, visitors to your domain name land at a **fraudulent copy** of your store, **compromising** your customers' **payment** and **personal information**.

Risk Scenarios #2

The email service you provide to thousands of users suddenly stops working.

You discover someone's transferred your domain name to another registrar without your notice or consent.

Your DNS configuration was modified, and **your** user's **email** is **delivered** to **someone** else's mail **server**.

Hours later, your registration is restored, but only after an exhausting and frustrating incident response effort.

Securing your Account #1

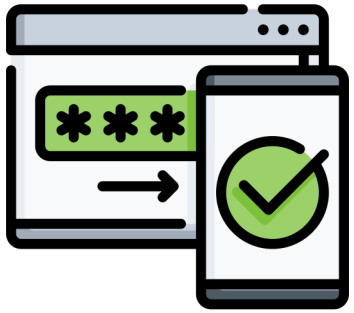
You should **take** account **security** very **seriously** because in almost every case, attackers will need access to your domain or provider’s account to steal your domain names.

These steps might **help** you to make **your account** more secure:

Have an up-to-date computer

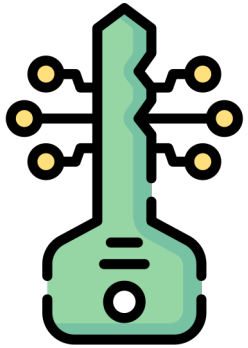
It sounds simple, but make sure you are updating your computer regularly and running a virus and malware scan. Try to avoid public computer, but if you have to clear forms, passwords, cache, and cookies. Make sure always to log off.

Securing your Account #2



Have an up-to-date account

Keep your account details up-to-date. Wrong address details or an old email address could cause problems.

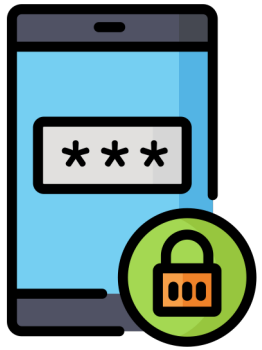


Use a reliable password

The longer the password, the harder it is to crack. Consider a 12-character password or lengthier. Mix it up. Use variations on capitalization, spelling, numbers, and punctuation.

Please don't write it down, send it via email, or tell anyone.

Securing your Account #3



Enroll in 2-factor authentication

If available at your domain name registrar, then enroll in 2-factor authentication. That will add an extra layer of security to your account.

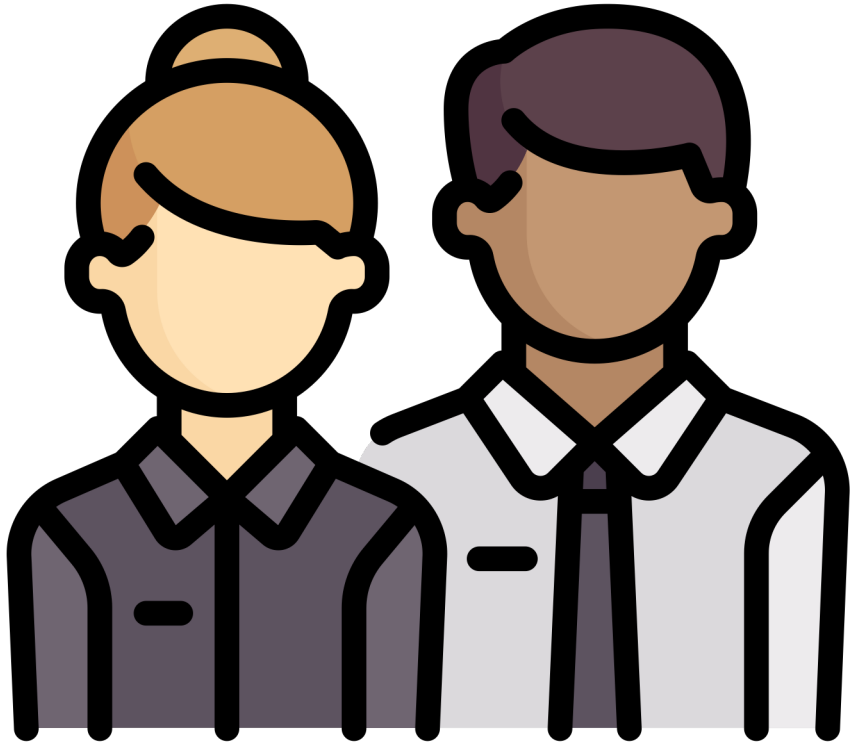
Protect your password

Never enter your password after following a link. It’s safer to type in the website to avoid phishing directly. Password manager, such as 1Password or LastPass, provides defense against phishing, and you don’t need to memorize every password.

Be the Registrant

In some cases, businesses have asked media agencies or web designer to set up a website or to register a domain name for them. That isn't per se a bad thing, but it's **crucial** to be sure **you** are the **owner** and **administrative contact**.

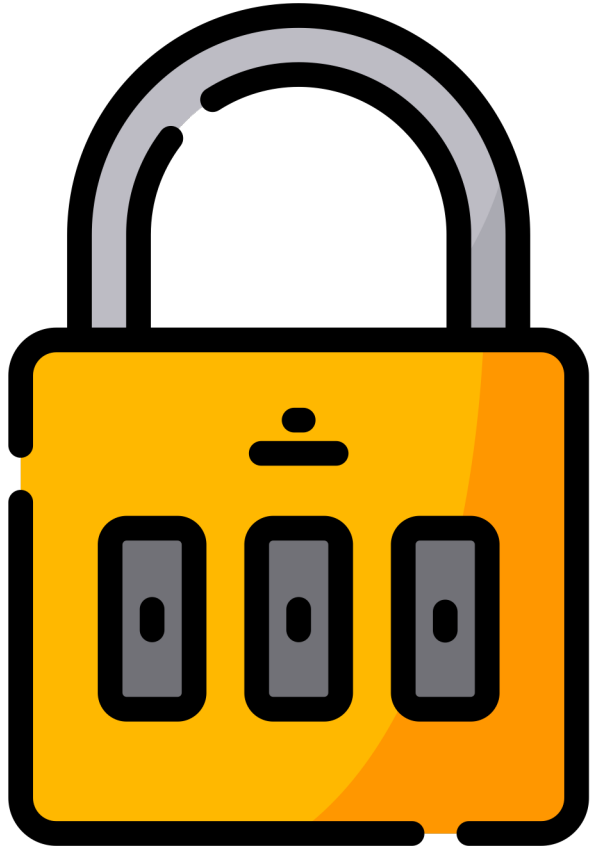
There are exceptional cases, such as WHOIS Privacy and Trustee Services, for ccTLDs. Still, recovering a domain from a 3rd party will get quite complicated if the ownership of the domain isn't clearly defined.



Authorization Code

In almost all **domain transfer** cases, it is necessary to have an **authorization code** (or auth code or auth info) to move from one **registrar** to **another**. This code is like a password and should be handled as such, therefore **avoid**

- … using the **same auth code** for all of your domains
- … **storing** auth codes **on your computer**
- … **sending** auth codes via unencrypted **email**



Protect your personal details

The WHOIS **contains** the domain **registrant details,** and it’s essential to **keep** these details **up-to-date**, because **otherwise** there is a **risk** to lose a domain name, due to policy violation or losing an old email account.

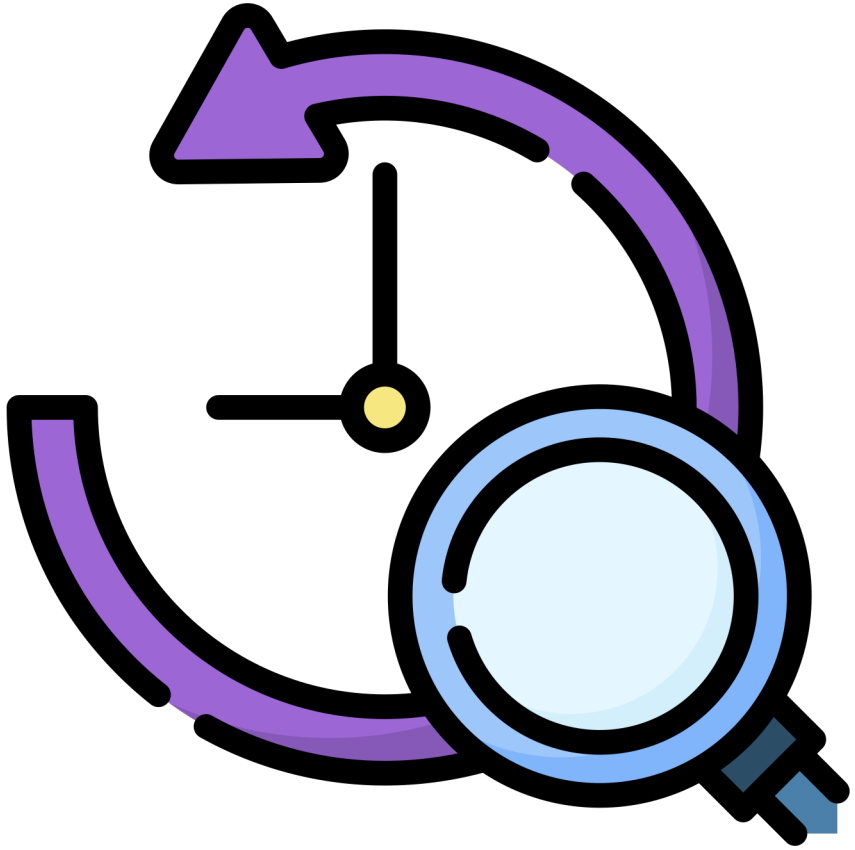
Privacy and **Proxy** from Registry and Registrar Services allow you to maintain a domain with WHOIS details other than your own.

That **prevents** that the 3rd parties can easily find out **your details** and abuse them.

Check Domain History

Even available domains can run the risk of causing legal trouble if the name is too similar to another company's trademark or used in shady business.

If you are unsure about that, then you may check if Google banned it on Google Safe Browsing, look up the domain on archive.org/web to see its history, and check the name on virustotal.com or consult a lawyer.



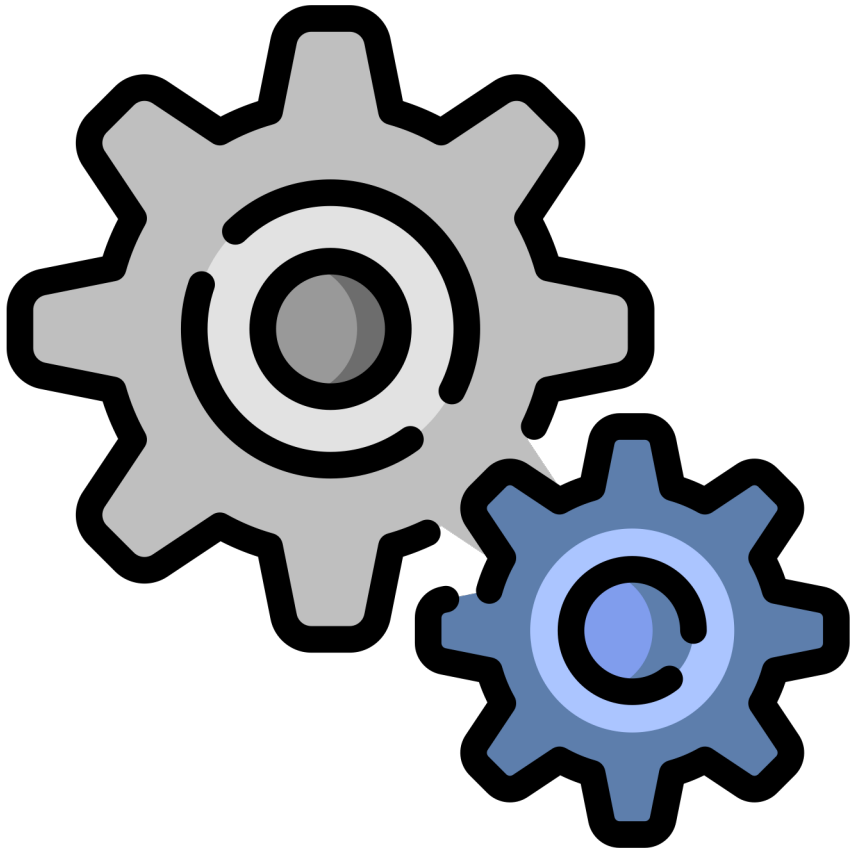
Set Transfer Lock

Depending on the TLD, each domain name may have domain status. The most common one is **ClientTransferProhibited** (colloquially called TransferLock), and it should always be set if available. That prevents a domain from being transferred from one registrar to another.

Many Registries are offering a Registry Lock Service. That will lock your domain name from Delete, Renew, Transfer and Update. It will add an even higher level of security.

MX Record

The mail exchanger (MX) Record specifies a mail server responsible for accepting emails. Like all records, the MX Record contains a Time to Live (TTL) value that indicates how long the DNS servers should use it before checking for updates.



Most **MX Records** have **TTL** of 3,600 seconds (1 hour). If someone gets access to your DNS configuration and change it, the attacker may redirect emails to update and transfer your domain name. Therefore, a higher TTL **might make sense**, such as **86,400** (1 day).

Thank you!