Cyber security

Your Home Is Your Castle?

Just as you always lock the door after leaving your house or for the night, you should ensure that your private digital data is safe. The totality of all technologies, processes and procedures designed to protect networks, computers, programs and data from attack, damage or unauthorized access is what we call cybersecurity. People nowadays have used to share precious personal data like phone numbers, credit cards or account details to companies and global corporations and we all expect it will be safe.

In terms of information technology, overall IT security often needs a complex of measures like cybersecurity itself and physical protection of possessions. In the past two years, many users fall into working from home or on the move but are you sure your data is safe?

Put It Into Practice

Talking about our daily routine, we can face most common cybersecurity threats like phishing, malware, ransomware, social engineering everywhere.

Though one of the biggest problems for reliable cybersecurity is the rapid and continuous evolution of many security risks and threats. For example, being an NFT owner is not only fun and trendy, but also responsible. It is important to know that the company you bought the NFT from operates the IPFS node. So one of the biggest vulnerabilities of NFTs is the case where the platform that is minting the NFTs ceases to operate. In such cases, you would lose access to the NFT, or the NFT could lose its value.

Just a handful of days ago, millions of dollars in the form of NFTs were stolen by an unknown. A hacker had compromised the official Instagram account for Bored Ape Yacht Club (BAYC) where he then posted a phishing link and transferred tokens out of users' crypto wallets.

Yet Other Useful Abbreviations

To protect your valuable data against all these potential risks, we have put together a set of recommendations:

- use strong passwords, a password manager and multi-factor authentication (MFA)
- seed phrase shall be given away under no circumstances,
- use hardware wallets. A transaction can only be carried out if it is confirmed by connecting the hardware wallet to a physical device and by an additional release, for example by entering a PIN,
- when buying NFTs, study the corresponding smart contract inside and out and use of fake crypto wallets,
- a solid VPN software system can be a solution.

Let us outline the main advantages of using a VPN (Virtual Private Network) to you:

- you can become almost anonymous online. A VPN encrypts a person's IP address which is like a digital fingerprint,
- bypass geo-blocking and
- as a nice side effect, your browser speed can be improved.

If you don't really want to spend your precious time protecting your NFTs, Magora can delicately do it for you. As an example, our IT architects have already succeeded in creating a robust environment and offered a high-speed VPN connection for a customer in Dubai. This particular task was to work out an architecture, create a robust environment and choose the appropriate hardware to provide a secure, stable, high-speed VPN connection using different protocols with flexible functionality and scalability.

Magora developers elaborated the whole environment with scalable architecture and fail-safe back-end seamlessly integrated with the mobile client to let the partner implement the front-end portion with their own team. The main point is that the high-load IT environment created with thousands of user operations per second works automatically and can be efficiently managed by the the client's administrator.

By combining advanced technologies and hardware and adding the magic of programming and administration expertise, Magora has created a unique, competitive, fully-fledged SaaS system. With a working version of the product our client has the opportunity to start a wide-ranging campaign to promote their own SaaS VPN environment on the market.