How to Protect Your Finances Against Cyber Attack

OCTOBER 26, 2021
By Deborah Boyland

Whether it's your investment portfolio, cryptocurrencies, or just your day-to-day banking accounts, protecting your finances from cyber-attacks is essential.
There are many digital threats to your financial accounts – but with the proper vigilance and awareness of how to protect yourself from threats, you can rest easy knowing your money and assets are safe.

The Internet has become a major part of our daily financial lives, from online bank accounts to apps for buying cryptos and stocks. In this article, I will help you understand the digital threats to your financial cyber security and offer 4 key ways to protect yourself and your money.

Understanding Threats to Your Financial Cyber Security

Bringing your finances online comes with many benefits, including convenience and accessibility. However, it also opens the possibility of your accounts becoming compromised by hacking attempts and cyber criminals.
When it comes to threats against your financial safety, there are 3 main types to be aware of:

1. **Malware/Ransomware:** Malware is the most common type of cyber attack. It is software designed to harm and exploit devices connected to the Internet. Ransomware is a specific type of malware wherein personal information or device safety is held at ransom by hackers.
2. **Malicious Bots:** Powered by malware, malicious bots are programs designed for hacking into a large number of accounts to gather information, send spam, and cause general cyber chaos.
3. **Phishing:** Phishing is a type of fraud wherein hackers pose as reputable companies and send emails that look official to unsuspecting consumers. These emails will contain links that, when clicked, deliver malicious bots or malware into your accounts or computer system.

Though there are other types of cyber-attacks as well, these 3 are the ones you are most likely to encounter on any given day.

4 Ways to Protect Your Finances Against Cyber Attack

Cyber-attacks can be frightening, especially when it is your financial safety at risk.
The first and most important step to protecting your finances digitally is to work only with financial service providers who are reputable and trustworthy. If you are unsure of an institution's commitment to risk mitigation or compliance, it's best to research their standing extensively.
With this in mind, here are 4 key tips for keeping your banking and financial accounts safe online:

1. Keep Your Password Clues Private

The Internet has become a cornucopia of knowledge for hackers. Information and clues about passwords and account names can be easily discovered through channels such as email and social media.
As such, it is critical to be aware of what you are sharing online and how it may lead hackers to figure out your sensitive information. To keep your password and account names private, you must practice good Internet safety by:

- **Using Private Accounts:** Whenever possible, you want to keep your online presence as private as possible – such as locking social media accounts so that only followers can see your posts. When you do post publicly, make sure these posts do not contain clues to your passwords.
- **Varying Usernames:** Many of us will repeat the same usernames again and again. Whether this is for simplicity or personal branding, it comes with great risk. Instead, you should vary your usernames when possible, especially those used for financial accounts.
- **Changing Passwords Regularly:** Hackers have become increasingly advanced in their methods. No matter how complex or safe you think your password is, there's always a chance a hacker can discover

it. To combat this, you should update and change your passwords regularly – this way, any hackers that have entered your accounts will be locked out swiftly.

2. **Always Use Verified Apps and Trusted App Stores**

Financial services of all kinds are available to you via your mobile device. This can add a ton of convenience when managing your finances, but it also increases the opportunities for hackers to catch you with a trick or fake app.

Avoiding this is as simple as sticking to verified apps purchased or downloaded through trusted app stores. Ideally, you should only be downloading your apps via stores such as the Apple Store or Google Play, which have many layers of protection to protect you from phishing and malware.

3. **Steer Clear of Phishing Emails**

Each of us likely has phishing scams hiding in our inboxes, hoping we are gullible enough to click them.

More often than not, if you use a major email provider these phishing emails will be automatically sorted out from your primary inbox. However, some may still make it through or even send notifications to your mobile device.

The key is to never click links within an email that you have doubts about. If you receive an email from a financial provider with a worrying message, your best bet is to contact the provider directly.

4. **Enable Multi-Factor Authentication**

Multi-factor authentication (MFA) is a log-in method that requires more than one verification factor to prove a user's identity. This often comes in the form of a phone number, backup email, or biometric verification (fingerprints, face scans, etc.).

MFA is one of the best ways for keeping your online financial information safe. Even if your passwords become compromised, a hacker is unable to access your accounts without the proper additional verification factors.

What's more, if they try and fail multiple times to figure out the secondary verification, your account provider will typically lock them out and contact you.

Final Thoughts

The safety of your finances is paramount – and the biggest threat to them is cyber-attacks.

With the help of the tips listed here, you can boost your Internet safety practices and ensure your information is safe at all times.