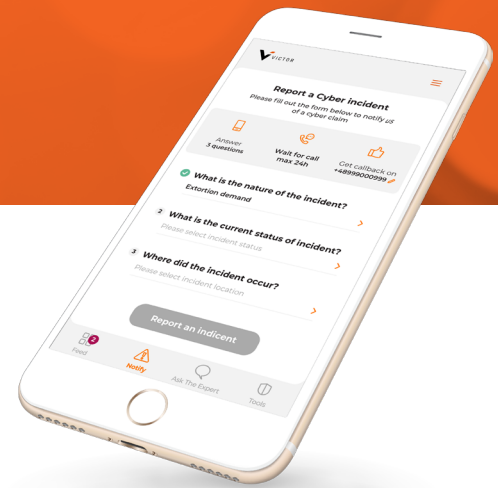


Victor Response: Frequently asked questions



Victor Cyber provides a full package insurance solution, competitively priced coverage and exclusive access to risk management services through our cyber incident mobile app, Victor Response. We want to make sure you have full access and maximize all tools available, so here are some of our FAQs to help you out.

I've downloaded the app, now what?

To register, all you need is your company email address and Victor Cyber policy number. This can be found on the second page of your policy doc under "Declarations." If your policy number contains a dash, ensure you include this. Following registration, you should then receive a confirmation email – make sure to check your spam. Your policy number will automatically update in the app when your policy renews, so there is no need to do this yourself.

I've already downloaded the old version of the app. Do I need to do anything?

In order to utilize all the latest risk management tools and benefits of the app, you'll need to download the latest version. This may happen automatically, but if it doesn't, you will be able to download manually through your phone's settings. You won't need to re-register, but you will need to change your password – just follow the forgotten password link on the login page of the newly updated app.

What counts as an incident/when should I report an incident?

If in doubt, it's better to reach out than to not. If you suspect something has happened, or could be about to occur, still report it as an incident within the "Notify" tab (you can select incident type as "other"), and a specialist from the Response Team will get back to you within 30 minutes or less with the best plan of action.

I've reported an incident through the app – now what?

1. One of the specialists from the Response Team will respond to you via telephone in 30 minutes or less. A specialist will run through the circumstances of your incident with you and advise you of any immediate steps that you can take.
2. A specialist will assess whether any other specialist services (forensic services, business resumption, legal etc.) are required to get you back to business as usual.
3. The team will email you a summary of the incident and an appointed partner vendor will contact you to determine the level of assistance required.
4. After mutually agreeing on the scope of work, the team will work to get you back to business as usual as quickly as possible.

Alongside this, a cyber claims specialist will be appointed who will proactively work with you throughout the lifecycle of the claim to advise you on steps that need to be taken.

Can multiple users have access to our account?

Anyone who is part of your organization can use the Victor Response app. They just need to download the app to their phone and use your policy number as the registration code. Victor Response is also used to deliver real-time threat alerts, as well as reporting claims – therefore it is worth considering who you would like to have access to this level of communication.

Can you have multiple policy numbers in the same app?

As these subsidiaries are listed under separated policies, you will need to register a new account for each policy number. To do this, log out of your account for the current policy then re-register with your other policy details.

An employee who had the app has left – now what do we do?

Get in touch with the internal support team at cyber@cfcunderwriting.com, and they'll be able to assist you with these access changes.

What risk management services are available and how do I access them?

Firstly, our real-time threat alerts will be your first backstop of protection. Through continuous monitoring of Victor policyholders' cyber threats and analysis of the latest cyber claims, the team is able to spot problems fast and send you critical alerts with guidance on how to rectify any issues.

You can then access the full range of risk management services by tapping "Tools" in the bottom navigation bar.

- **Phishing simulation** – this is a simulated email campaign that goes out to members of your team whose credentials are most vulnerable. These emails look like phishing emails in order show users how easy it is to fall victim and to raise awareness of this criminal tactic.
- **Dark web monitoring** – this tool scours the dark web for information relating to your business, including corporate login credentials and other breaches of sensitive data relating to your domain name.
- **Deep scanning** – this service actively scans the external client network footprint to identify claims-correlated vulnerabilities that lead to cyber-attacks and ransomware.

What is Ask the Expert? What sort of questions could I ask?

"Ask the Expert" is a direct route for any technical questions you might have. It puts you in communication with a specialist team who will respond within 48 hours and help with cyber risk mitigation, best practices and cybersecurity services on offer. Please note, this service is not for policy coverage questions or renewal queries. These will still need to go to your broker.

Some of our frequently asked questions are:

1. What is two step authentication and why might we need it?
2. How can you help us in the event of an incident?
3. How can we prevent attempts to gain unauthorized access to corporate accounts?

Do I need to supply any other information for the tools to work?

Nothing else needs to be supplied for the tools to be activated and to start working.

Do the tools cost anything extra?

No. Access to the app is included for free to every Victor Cyber policyholder.

I've received a real-time threat alert about a data breach – do I need to do anything?

If you get an alert, make sure you read the full detailed report that will accompany the notification. Each alert will be different and may have different action. If in doubt, please reach out via the “Ask the expert” chat function.

The most common advice provided is:

1. If a password is included in the breach, change all corporate passwords for the user where possible. Ensure you have a robust password policy in place and implement 2FA for all externally-facing accounts. Educate users about the risks of password reuse and monitor the accounts closely.
2. If only address or phone numbers are involved, be aware that the affected users may be at higher risk of being targeted in a phishing campaign. Alert these users, monitor their accounts closely, and educate them on ways to spot a phishing email.

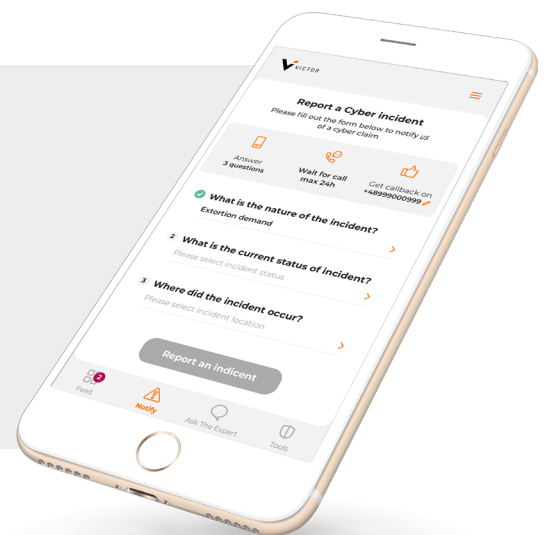
**The Victor Response app is available
on the App Store or Google Play.**



Scan for Apple devices



Scan for Android devices



Visit victorinsurance.com to learn more.

[View our demo](#) for guidance on how to navigate through the app and utilize its tools and services.

This document is for illustrative purposes only and is not a contract. It is intended to provide a general overview of the program described. Please remember only the insurance policy can give actual terms, coverage, amounts, conditions and exclusions. Program availability and coverage are subject to individual underwriting criteria.

© 2023 Victor Insurance Managers LLC | 80091

Victor Insurance Services LLC in MN | DBA in CA and NY: Victor Insurance Services | CA Ins. Lic. # 0156109