CYBER SECURITY

Z SOFTWARE

Z Software has partnered with leading Cyber Security Solutions to ensure that our customers are aware of their Cyber Security risks and together tailoring solutions to cater for every aspect of awareness from training, protection, and monitoring.

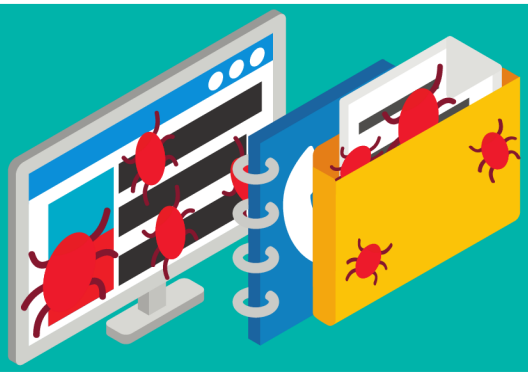
What is Cybercrime?

Cybercrime is "a crime where a computer is the object of the crime or is used as a tool to commit an offence."

The offender may use a device to gain access to the targeted user's personal details, confidential business information, government data, or to disable a device. Selling or eliciting the content mentioned above online is also considered a cybercrime.

Over the past few years there has been a significant increase in cybercrime targeted at the SME market. There are two factors contributing to this rising epidemic.

First, is the rise of crypto currencies, which has enabled anyone in the world to be paid a sum of money without being identified or held accountable (e.g. ransomware).



Second, is the increased focus on security by the enterprise sector, meaning that targeting many small businesses has become far more effective than attacks aimed at high-security large companies

Significantly reduce your business' cyber risk with these steps

Assess your pharmacy's cyber security risk

Complete our online health check to access your pharmacy's security risk score.

Implement the easy to follow cyber security framework

With your risk dashboard you can then work through areas that are putting your pharmacy at risk. Framework assists you implement cyber security policies with our policy templates along with actionable checklists.

Deliver online training to your team

Utilise our short engaging online training videos for your team and measure their engagement and compliance over time. It will identify those members who are a potential risk to your pharmacy and offers them targeted training.
Phishing simulations throughout the year also aim to educate team members. With access to multiple campaign templates, you can send out simulations and then gain insight into team members email vulnerabilities.

Patch any holes in the network infrastructure of the business

Now that you have a better understand of the gaps in the network infrastructure you can now work on patching the holes. This might include installing network firewalls, patching equipment along with identifying all the endpoints on your network and installing antivirus and ransomware protection on them.

Constant monitoring of network traffic, devices and cloud services for any suspicious behaviour that might be trying to infiltrate your pharmacy

Integrating all security data within your network looking at your firewall, endpoints, cloud workloads, dark web breaches and compromised credentials, our Security Operations team analyses attack patterns and alerts your team as soon as possible when suspicious activity is detected within your pharmacy.

Z Software along with our partners have created the following programs to assist pharmacies with various components of the 5 steps we have identified to strengthen your cyber security.

	Cyber Alerts	Cyber Protect
Healthcheck	X	X
Risk Dashboard	X	X
Cyber Framework	X	X
Awareness Posters	X	X
Online Team Training	X	X
Network Firewall	X	X
Firewall Alerts	X	X
Phishing Simulations	X	X
Firewall Monitoring	X	X
Endpoint Monitoring		X
Email Monitoring		X
Instance Monitoring		X
Dark Web Breaches		X
Special Operation Team		X
Cyber Remediation		X

Z SOFTWARE