



# Managed Security Services

You have a business to run; let us protect your technology.

## OUR PARTNERS

mimecast

SOPHOS

Microsoft

PERCH

CISCO Meraki

CYLANCE

CISCO

Today's threat landscape is ever evolving, and many companies are left unprotected. Let PSM Partners take the worry out of your IT Security with our expertise and secure solutions. We are focused on a layered security approach backed by our Chicago-based Network Operation Center team.



Threat Management

- Advanced A/V with EDR
- Spam and Phishing Protection
- Web security and DNS Protection
- Intrusion Prevention System
- UTM/NGFW Firewall

Vulnerability Management

- Endpoint detection and response
- Security Operations Center
- Intrusion Detection System

Full Service Desk Support

- Data loss prevention
- Vulnerability Scanning
- SIEM Log Collection
- Risk assessment and Gap Analysis
- Patch Management

## CONTACT US

(312) 940-7830 | sales@psmpartners.com  
www.psmpartners.com



209 W. Jackson Blvd, Suite 903  
Chicago, IL 60606



### Utilize a firewall

A firewall monitors and controls incoming and outgoing network traffic. To ensure your computer is safe make sure your Windows 10 firewall is turned on. Many vendors and some internet service providers (ISPs) offer integrated small office / home office routers that also include firewall features.

### Advanced antivirus (A/V's) with endpoint detection and response

Next-Gen AI driven antivirus that outperforms and out protects traditional A/V's. This product not only is built on cloud AI to spot threats before traditional A/V's but it also contains advance protections such as sandboxing suspicious processes, disabling the threat and source analytics.

### Multi-Factor Authentication (MFA) Gmail/Yahoo/Outlook

Multi-Factor Authentication is a security enhancement that allows you to present two pieces of evidence – your credentials – when logging in to an account. MFA has become a security and compliance standard for almost all cloud platforms and provides an extra layer scrutiny. MFA is especially important for email security to protect your accounts. If MFA is not currently set up, you should enable it immediately.

### Make sure that passwords are protected.

Use passwords that are not easy to guess. They should be at least 8 characters long with the following – 1 capital, 1 lowercase, and at least 1 number. Example – Hu0xtfPjs. This should be done for all your online accounts including your computer as well. Don't reuse the same passwords for multiple accounts.

### Keep all computer and antivirus software up to date.

When you update your software, you'll get the latest fixes and security improvements, helping your device run efficiently and stay protected. In most cases, restarting your device completes the update.

### Don't open suspicious emails and/or links.

Scammers use email or links to trick you into giving them your personal information. If you receive an email from someone you don't know, or a suspicious email address, do not open or click on the message. They may look like they're from a bank, a credit card company, a social networking site, an online payment website or app, or an online store. This could cause malware to be installed or take you to an unsafe website.

## CONTACT US

(312) 940-7830 | sales@psmpartners.com  
www.psmpartners.com



209 W. Jackson Blvd, Suite 903  
Chicago, IL 60606