



Apex Managed Services

Enterprise-grade cybersecurity for growing businesses.

CYBER RISK REPORT

Noxantis

noxantis.com

50

OUT OF 100

High Risk

PREPARED

August 5, 2026

(555) 018-2947

security@apexmsp.example

EXECUTIVE SUMMARY

Cyber Risk Report

Noxantis
noxantis.com

Significant vulnerabilities were found that require prompt attention.



Higher score = better security

High Risk

● Email Security

● SSL & Website

● Dark Web

● Open Ports

● Domain

CRITICAL FINDINGS

6

issues need attention



EXPOSED PORTS

0

no open attack surface



BREACHED ACCOUNTS

0

no credentials exposed



SECTIONS AT RISK

3 / 5

areas with open issues





Email Security

-30 pts

✗ FAIL



No DMARC Record Found -15 pts

FAIL

This domain has no DMARC record. There are no instructions telling email providers what to do with fake emails.

WHY THIS MATTERS

Even if SPF and DKIM are set up, there is no final rule to block fake emails. Scammers can still impersonate this business.

WHAT TO DO

Add a DMARC record to your domain. Start with 'p=none' and a report address, then switch to a stricter setting over time.

DMARC stands for Domain-based Message Authentication, Reporting and Conformance. It is a rule that tells email providers what to do with emails that fail security checks.



No SPF Record Found -10 pts

FAIL

This domain has no SPF record. Any email server in the world can send emails pretending to be from this domain.

WHY THIS MATTERS

Scammers can easily send fake emails that look like they came from this business. This puts clients and staff at risk.

WHAT TO DO

Add a TXT record to your domain settings that lists which email servers are allowed to send mail on your behalf.

SPF stands for Sender Policy Framework. It is a rule in your domain settings that controls which email servers are allowed to send mail using your domain name.



DKIM Not Found

-5 pts

FAIL

No DKIM record was found for this domain. Emails sent from here do not have a digital signature.

WHY THIS MATTERS

Without a signature, email providers have no way to verify that emails really came from this business.

WHAT TO DO

Get the DKIM record from your email provider (such as Microsoft 365 or Google Workspace) and add it to your domain settings.

DKIM stands for DomainKeys Identified Mail. It adds a hidden digital signature to emails so the receiver can verify they are genuine.



Not on Any Email Blacklists

PASS

This domain's mail server was not found on any of the major email blacklists that were checked.

Checked against: Spamhaus, Barracuda, SpamCop



SSL & Website Security

-10 pts

✗ FAIL

Issuer · GoDaddy.com, Inc.

Expires · Sep 14, 2026 (40 days)



Certificate is Valid

PASS

This website's security certificate is valid and doesn't expire for more than 30 days.

SSL stands for Secure Sockets Layer (now called TLS). It is the technology that creates an encrypted connection between a visitor and a website, shown as the padlock icon in a browser.



No Website Security Headers Found -5 pts

FAIL

This website sends no security rules to browsers at all.

WHY THIS MATTERS

Without these rules, browsers have no extra protection turned on for this site. Visitors are more exposed to web-based attacks.

WHAT TO DO

Set up security headers through your web server or content delivery network. Many hosting platforms have a one-click option for this.

HTTP Security Headers are instructions a website sends to a browser. They switch on built-in browser protections, like stopping the site from being secretly loaded inside another page.



Website Does Not Redirect to Secure Version

-5 pts

FAIL

Visitors can reach this website over plain HTTP without being sent to the secure version.

WHY THIS MATTERS

Visitors using the plain HTTP version have their information unprotected. Passwords, form data, and cookies can be read by others on the same network.

WHAT TO DO

Set up a permanent redirect from HTTP to HTTPS in your web server or hosting settings.

HTTPS stands for HyperText Transfer Protocol Secure. It is the secure version of a web address. HTTP without the S means the connection is not encrypted.



Dark Web Exposure

✓ PASS



No Leaked Accounts Found

PASS

No email addresses from this domain were found in any known data breach databases.



Open Ports & Network Exposure

✓ PASS



Remote Desktop is Not Exposed

PASS

Remote Desktop access (port 3389) is not open to the public internet from any address detected for this domain.

RDP stands for Remote Desktop Protocol. It is a tool that lets someone control a computer over the internet, as if they were sitting in front of it.



File Sharing Port is Not Exposed

PASS

The file-sharing port (445) is not open to the public internet.

SMB stands for Server Message Block. It is a protocol that lets computers on a network share files and printers with each other.



Domain & Infrastructure

-10 pts

✗ FAIL

REGISTRAR

GoDaddy.com, LLC

DOMAIN AGE

3.1 years

EXPIRES

June 12, 2027



IP Address Has Abuse Reports

-10 pts

FAIL

The IP address hosting this domain's website has recent abuse reports — things like hacking attempts, spam, or malware activity — logged in threat-intelligence databases.

WHY THIS MATTERS

Sites hosted on flagged IP addresses can get blocked by corporate firewalls and security tools, and on shared hosting, one compromised neighbor on the same IP can drag others down with it.

WHAT TO DO

Ask the hosting provider about the abuse reports. If this is shared hosting, consider moving to a dedicated or better-vetted IP address.



No Browser Safety Warnings

PASS

Google Safe Browsing has no warnings for this domain. It is not flagged as a phishing or malware site.

Google Safe Browsing is a service that checks websites for phishing, malware, and harmful content. It powers the safety warnings shown in Chrome, Firefox, Safari, and other major browsers.



Domain Registration is Paid Up

PASS

This domain registration is active and will not expire for at least 90 days.

Priority Actions

- 1 No DMARC Record Found
-15 points · Email Security
- 2 No SPF Record Found
-10 points · Email Security
- 3 IP Address Has Abuse Reports
-10 points · Domain & Infrastructure
- 4 DKIM Not Found
-5 points · Email Security
- 5 No Website Security Headers Found
-5 points · SSL & Website Security



Apex Managed Services

Ready to fix these issues?

Enterprise-grade cybersecurity for growing businesses.

 [Get in touch](#)

📞 (555) 018-2947

✉ security@apexmsp.example

This report was generated on August 5, 2026 using data collected from publicly accessible sources and threat intelligence databases. Findings represent the security posture observed at the time of assessment and may change. This report is intended for informational purposes only and does not constitute legal or compliance advice.

Visits to this report are logged (IP address and approximate location) and are visible to Apex Managed Services.