

# DESKTOP-7Q2 · Windows 11

Example customer · Scanned 4 October 2026

1

Critical

1

High

1

Medium

## Summary

This PC has one urgent problem — a disguised program talking to a known malicious server — and two settings that make it easier to attack. Fix the critical item first; the other two take a few minutes each.

### 1. Connection to a known-malicious IP address

Critical

#### 📌 NETWORK CONNECTIONS

```
> svch0st.exe → 45.137.21.53:443
> 45.137.21.53 is listed on public botnet blocklists
```

**What it means:** A program on this PC is talking to a server known for malware. The program name imitates a Windows component (svchost.exe), a common trick.

#### How to fix it:

1. Disconnect the PC from the internet until the program is removed.
2. Run a full Microsoft Defender scan (Windows Security → Virus & threat protection → Scan options → Full scan).
3. Remove the scheduled task that starts the program (Task Scheduler → \Microsoft\Windows\UpdateSync).
4. Change passwords used on this PC from a different, clean device.

## 2. Remote Desktop is open to the network

High

### 📌 OPEN PORTS & EXPOSED SERVICES

- > TCP 3389 listening on all interfaces (TermService)
- > Network Level Authentication: off

**What it means:** Anyone who can reach this PC can try to log in. Exposed Remote Desktop is one of the most common ways ransomware gets in.

#### How to fix it:

1. If you don't use Remote Desktop: Settings → System → Remote Desktop → Off.
2. If you do: turn on Network Level Authentication and only allow access through a VPN.
3. Use a long, unique password for every account that can sign in.

## 3. Windows Firewall is off for public networks

Medium

### 📌 WINDOWS SECURITY SETTINGS

- > Firewall (Public profile): off

**What it means:** On café, hotel or airport Wi-Fi, other people on the same network can reach services on this PC.

#### How to fix it:

1. Windows Security → Firewall & network protection → Public network → On.

Reviewed by the Keepvik team. Findings are based on measurements taken on the computer at the time of the scan. No scan can find every threat.