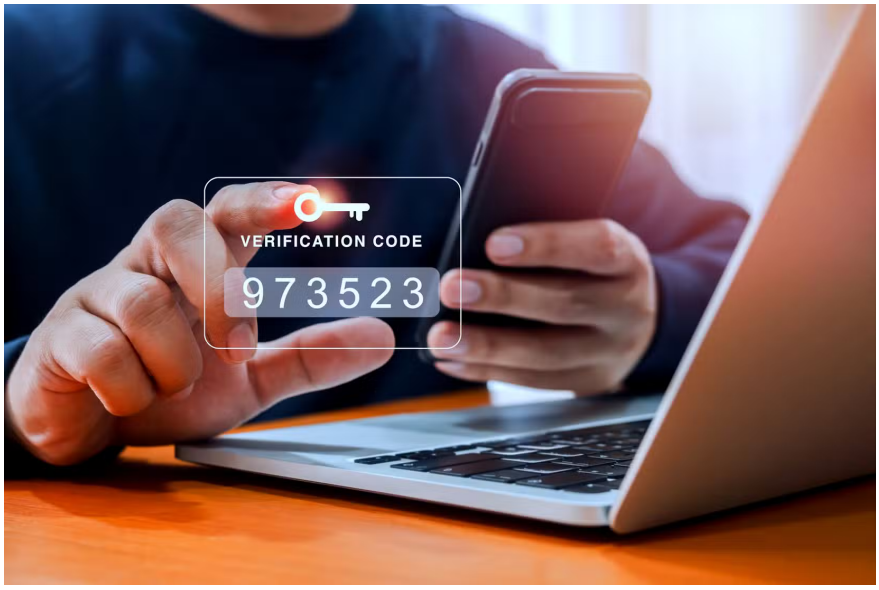
4 Security Steps to Follow When Using Remote Access Applications

Remote access applications are great for controlling your PC when you're not sitting directly in front of it. However, remote access applications are often a prime target for hackers, but you can thwart their attempts by making a few security adjustments.

1. Enable two-factor authentication for remote access applications



Modern powerful computers can crack a 7-letter password in seconds. Using a password tool to generate a strong passphrase will increase this time exponentially, making it more resistant to brute force attacks.

Unfortunately, having a strong password is no longer enough, as attackers often compromise your credentials through other means.

1. Convincing phishing emails
2. Exploit weaknesses in the application's password security design (VNC and Windows RDP have been notorious for this in the past)
3. Hack into servers to steal credentials stored on corporate databases

There's an easy way to make sure you're not at the mercy of simple password authentication: Two-factor authentication (2FA). Many remote access solutions like TeamViewer make it easy to enable 2FA, which can send an email or text message to your mobile device to check if you're logged in. The second verification

method makes it much harder to break in than using a password alone.

2. Update Remote Desktop software regularly

Of course, a password won't stop an attacker if the software itself is vulnerable, which is why it's so important to install regular security updates for remote desktop.

Things move fast in the tech world, and if an app hasn't been updated in over a year, you're asking for trouble. If you're still running NoMachine version 8.02 when version 8.14 is out, hackers will try any of the vulnerabilities listed in the old patch notes.

Turn on automatic updates for peace of mind, but if you can't, put it on your to-do list to check regularly. That's the point!

3. Restrict remote access via whitelist

Why give bad guys a chance to unlock when you can completely destroy that chance? Many remote access apps let you restrict who can connect in the first place.

You might think that unless you are a celebrity or a tech giant, no one would target your humble PC. However, attackers often use port scanning on entire IP blocks to find easy clues. If you have a remote server exposed to the wider Internet, it is not secure.

Luckily, you can use IP address whitelisting to check who's knocking on your door. Remote control apps like AnyDesk let you set which devices you trust, while other remote access apps like Splashtop let you specify which IP addresses you want to recognize.

If whitelisting via IP address, take precautions so you don't accidentally lock yourself out.

A client device can have a dynamic IP address that changes without warning. Suddenly, it is no longer on the whitelist and you have blocked yourself. Here are some ways to make sure you can edit the whitelist when needed:

1. Specify a wider subnet range to account for locations you frequently visit, such as your home or office, using the handy subnet calculator
2. Have physical access to the remote computer
3. Have web access to the vendor portal (e.g. logmein.com)

4. Connect to VPN before using remote control

If you're using a public Wi-Fi hotspot—or any network that isn't yours—to connect to remote desktop, your activity isn't secure. That's because your traffic is being routed through someone else's hardware.

One solution is to connect to a VPN before starting your remote session. VPNs provide end-to-end encryption and protect you from eavesdropping. You should choose one from this list of the best VPN services.

For those who host their own remote access servers – for example, RealVNC, Windows RDP, or Chrome Remote Desktop – there's a better solution. This method lets you take advantage of the VPN's superior security standards to block outsiders.

Here is the core of the setup:

1. Restrict remote access software to only accept connections from your home network (or the network you're using) and deny everyone else.
2. On your home network, set up your own VPN with WireGuard, Tailscale, or a service built into your router.
3. When you want to access remotely, tunnel into your home network by connecting to the VPN. Now you will be able to connect to your remote PC as if coming from your local network.

The downside to using a VPN is that it often slows down your streaming and requires some setup. But it's the gold standard for remote access to corporate and university networks for a reason.

By the way, you're not limited to just one technique. Combining several of the security steps above will turn your remote PC into a well-protected fortress.