Part of our Privacy & Security Series

NOS Online Privacy & Security

Brought to you by National Online Safety®

www.nationalonlinesafety.com

What you need to know about...

REMOTE ACCESS & REMOTE DATA DELETION

What are they?

'Remote Access'

Remote access, as the term suggests, refers to the ability to access a computer, such as a home computer or a machine that's connected to a school's network, from a remote location. Remote access can be set up using a local area network (LAN), a wide area network (WAN) or a virtual private network (VPN), and once established, it gives you full control over the device you're 'remoting' to. You can then run any applications and even open files on the machine.

'Remote Data Deletion'

Remote data deletion is related; this is a security feature that allows a network administrator, for example, to send a command that deletes data on a computing device. It is primarily used to erase data on a device, such as mobile phone or laptop, that has been lost or stolen so that if the device falls into the wrong hands, the data won't be compromised.

Know the Risks

Cyber-scams

Some popular scams employ remote access tools in order to infect your PC with malware and obtain financial details. These typically appear in the form of phone calls, where a company warns you that your computer has a security problem and promises to remote-in and fix it.

Privacy concerns

If your child is using remote access software and is also allowing others to access their computer, it could mean that they're potentially providing the remote user with access to sensitive information, such personal images or videos or even financial details.

Permanent loss

Remote deletion is a great way to ensure that if your device is lost or stolen, that the data cannot be compromised by others. However, if the data isn't backed up elsewhere and a remote wipe is completed, this can lead to permanent data loss which is irrecoverable.

Hacking risk

While many, typically paid-for remote access tools will encrypt remote sessions between the local and remote devices, some services don't offer such protections. This could leave any information passed over the service open to hacking and the theft of personal and private information.

Safety Tips

Protect your devices

Always protect your devices with the most up to date security software. While both Windows and macOS have built-in protections against malware threats, it's recommended that you implement additional measures, from firewalls to two-factor authentication (2FA).

Avoid public WiFi

If you or your child are using remote access software, it's always best to avoid using a public Wi-Fi hotspot. These are often open networks that are typically unsecure by nature, and prime locations for cybercriminals to gain access to your devices.

Read the small print

When you or your child are installing remote access software, it's important you know what you're downloading so that you know that your data will remain safe. You must make sure the service offers built-in encryption, complies with regulations (such as GDPR), and that it's fully compatible with the PC and mobile devices that will be connecting to it.

Backup data

You're never going to be warned prior to unexpected data loss, which is why it's critical to back up any important data - particularly if data ever needs to be wiped remotely. While this data can be backed up in the cloud, it's always advisable to have a physical copy too.

Conversation Tips

Talk about privacy

Remote access has long been a target for cybercriminals, and even if they don't feel at risk, it's important your child is aware of the security issues and knows how to maintain strong online privacy, be it through the use of strong passwords or multi-factor authentication. Always ensure they know never to let an unauthorised third-party gain remote access to their system.

Understand their usage

Always ensure you know what your child is downloading or how they are using their devices. If they're using remote access tools, it's important you're confident that it's secure. Talk to children about potentially using a reputable VPN to offer extra security and making their computers less vulnerable to hackers.

Our Expert

Carly Page

Carly Page is an experienced and highly respected freelance technology journalist, editor and consultant. Previously the editor of tech tabloid The INQUIRER, Carly now works as the news editor for Computer Shopper and IT Pro and writes for a number of publications including Forbes, TechRadar, Tes, The Metro, uSwitch and WIRED.