

REMOTELQ™ SAFETY TIPS



FOR SECURE ACCESS AND PROTECTION

HARDENED ENCRYPTION

Cattron's RemotelQ website uses a HTTPS - Hypertext Transfer Protocol Secure - encryption connection to the cloud. It protects page authenticity on all types of websites, secures accounts and keeps user communications, identity, and web browsing private. Whether you are accessing data via your mobile phone, tablet or home office computer, your data's integrity and privacy are protected.

PASSWORD PROTECTION

If locked out of your account, you can set up a new password on the login page following the prompts. Cattron will never ask you for your password, and any email communications you may receive will come from @cattron.com or @remoteiq.com.

PRACTICE SAFE BROWSING

Never leave yourself logged in to a public computer. Free Wi-Fi networks at cafes and restaurants are not secure. Have a strong password set up on your devices. This will provide an additional layer of security should your device become lost or stolen.

KEEP YOUR PASSWORD SECURE

Always select a strong password. RemotelQ requires highly complex, case-sensitive passwords that include symbols. Never store your passwords in the open, write them down on sticky notes or share your password with anyone. And never set up passwords for a group to share. This increases the opportunity for hacking or phishing attacks. It is also recommended to change your password frequently.

For questions about RemotelQ, email us at Request.NA@cattron.com.