

G:M Top Security Basics

1

Make Authentication Your Fortress

Passwords are important but they aren't the be-all and end-all. Have you thought about using two-factor authentication to prove the users identity?

Make sure your data is backed-up using the 3-2-1 rule - 3 total copies, 2 different mediums, and 1 off-site copy. If it's not backed-up make sure you know that.

2

Have a Plan B

3

Make Updates Your Priority

Out-of-date software makes you vulnerable to attack, so make sure security patches and fixes are applied instantly, and as automatically as possible.

Humans are often the weakest link in the security chain so make sure your employees are educated on what a social engineered attack or phish looks like so they don't give up sensitive information.

4

Don't Give Up What is Yours

5

Make the Rules Clear

Make sure all your employees are educated on security policy and understand the implications of their actions on the wider organisation.

Managing devices inside your network is one thing but what happens when devices are outside your network. Make sure you have an MDM solution that enables you to manage all your devices and take control when you need to.

6

Make MDM Your Watch Word

7

When Was Your Last Audit?

Make sure to ask yourself and your team the difficult questions about your security plans and look to constantly make improvements where you find vulnerabilities. Don't wait to be a victim of cyber crime.

Stay in touch with changes in working practice for example, BYOD and have a plan ready before any damage is done.

8

Keep Looking Forward

Want to understand how to make your environment more secure?
Contact a consultant today.

