AIRO

TOP 10

Essential Cybersecurity Measures for Safe Remote Working

Staying safe online isn't just for people who are worried about getting hacked; it should be the first priority for anyone who wants to run a successful, safe business and keep their clients both secure and happy. It's easy to get caught up in the loop of 'it could never happen to me', and we're here to tell you it could both happen to you and it's very easy to stay safe online with just the tiniest adjustments to your day to day routine.

Here are the **top ten essential cybersecurity** measures you can take while **working remotely:**

1. **Make sure users have updated their PCs.**
   Most cybersecurity threats happen when vulnerabilities are found in existing software, hence why Windows keeps rolling out regular updates to address these vulnerabilities.

2. **Make sure users have an active and updated antivirus software.**
   Similar to regular updates, it's easy to just download an antivirus software and leave it running in the background without checking on it. For maximum safety, make sure your antivirus is up to date.

3. **Teach users to use complicated passwords at least 12 characters in length.**
   By using one symbol, one uppercase letter, and one number, it's harder for hackers to break into your account.

4. **Get your users into the habit of using password managers.**
   Password managers such as LastPass or Bitwarden can generate a complex password for you, without you needing to remember it; it's the easiest way to stay safe online without running the risk of saving your passwords into your browser.

5. **Encourage your users to keep different passwords for each website.**
   This way, even if one of their accounts is compromised, it doesn't affect the rest of their accounts, and with a password manager, they don't even need to remember all of their different passwords.

6. **Teach address bar safety.**
   Does the website you're on or about to submit sensitive information to have the proper safety protocols? if there's a little lock symbol in the address bar, you're good to go; if not, find a better way to send your confidential data, and definitely don't enter your credit card information in. A missing lock symbol means that the website doesn't have the best security measures; better safe than hacked!

7. **Keep your own systems' certificates up to date.**
   Similar to the above: if your internal security is lacking, your external security (your users) is going to suffer in the long-run.

8. **Teach your users to never access websites with expired certificates.**
   Although browsers now warn users in advance that the website they're about to visit has an expired certificate, it still allows you to go through if you really want to. Make sure your users know the massive risk an expired certificate poses.

9. **Make sure that your email systems have anti-phishing, anti-spam, and anti-malware scanning enabled.**
   This limits the risk that your users will get caught out by a particularly convincing phishing email - and they are getting more sophisticated by the day!

10. **Ensure email domain has SPF/DKIM measures.**
    This one's just self-explanatory: the biggest problem with cybersecurity tends to be that human error is impossible to predict, so give your users as little opportunity for error as possible.

Want to know more about staying safe?

Our **blog** updates regularly with the best tips for staying safe online. Head on over to our **website** at airosoftware.com/latest-trends to read our latest posts.