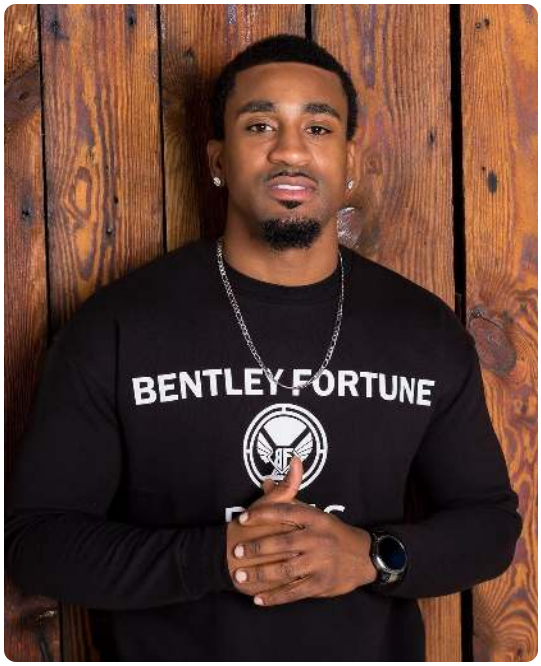
Securing Your Computer

How to Keep Work Computers Secure

About The Author

Marwyn Allen is an Information Security enthusiast and businessman. Marwyn Allen, originally born and raised in Jamaica came to America in 2011 to pursue his business and education goals. Marwyn has worked in corporate America for over 10 years with brands such as Amazon and Truist in various roles such as Shipping Manager, IT Business Analyst, IT Support Engineer, Cyber Incident Management and Senior SOC Analyst.

Marwyn is also a serial entrepreneur that owns a consulting agency, financial agency, Information Security firm and an events business.



About The Author

Marwyn along with his team has helped to build over a dozen brands using the skills of business management and expert business automation. Marwyn is a lover of nature, wildlife and true crime junkie.

Marwyn spends most of days during the week building his various brands, spending time with his family, working out in the gym and binge-watching documentaries. **You can find a list of Marwyn's credentials and portfolio below:**

About The E-Book

This book was created with the intention of providing every day adults, small to medium size business owners and beginner Information Security students with general knowledge of threats, threat actors, scam techniques and ways to secure themselves and their businesses online.

The information given in this book is ever changing due to the nature of the information security industry. Readers are advised to do their own research and validation when implementing any information security protection and or policies. Allen's InFoSec agency is not responsible for any damage, harm or loss of finances, resources and or life caused due to any information displayed in this book.

How to Keep Work Computers Secure?

When working to keep data and passwords safe within company computers, employers need to be proactive in ensuring that employees are not putting them at risk. There are risky behaviors that employees do on work computers that a company needs to look at limiting.

Risky Employee Behavior

* Unauthorized use of programs. When employees use unauthorized programs on company computers, it can lead to loss of data for the company.

* Corporate computers used without supervision.

* Transfer of files from work computers to home computers.

* Employees sharing their password with other employees.

* Employees gaining access to unauthorized network facilities.

There are ways to implement procedures within the workplace to reduce these risky employee behaviors and keep your data safe.

How to Prevent Data Leaks?

1. Have clear policies that all employees are aware of. This includes stating what belongs to the company when an employee leaves a job. Make it clear from the start that all documents and data created by the employee are property of the company even after employment has been terminated.

2. Make sure staff are aware of data protection policies. From day one of employment you should have employees go through training classes on data breaches. Then doing it regularly with all employees throughout the year will not only confirm how committed you are to protecting data, but will also remind employees of what you expect as well as keep them up-to-date on any new practices you have put into place.

Make sure the training includes software and tools that are used to protect data. Also inform employees of the company policy of using personal devices when completing work.

3. Use employee contracts. Making new employees sign a contract which includes policies on codes of conduct as well as data ownership helps protect companies. Letting employees know not only what you expect of them, but also what belongs to the company as well as the consequences of not following these rules, will go a long way to keeping your company data safe.

4. Only allow the appropriate people to have access to specific data. Not everyone is going to need all data, so only granting access to the appropriate team members helps keep the data from getting into the wrong hands. You can keep this organized so you know who has access to what with a spreadsheet that lists each employee's access to specific apps, tools, and information. This will also help you cancel roles when necessary to the appropriate information.

5. Report suspicious activity. No one wants to be the snitch on the job. But if you encourage it of all employees and give them a way to report suspicious activity anonymously, then people will be more likely to report. Train everyone on how to recognize things like phishing schemes and how to speak up to the appropriate person in these matters.

You might not be able to completely prevent a data breach, but you can put things in place that can help you keep data safe. Most importantly, having your finger on the pulse of everything within your business will go a long way to ensuring that data remains secure. The longer you wait to address a situation, the bigger the problem is going to be.

Thank You!

You have reached the end of this e-book, we hope you enjoyed the summary of contents that we've put together for you. We are always looking to improve our content so please feel free to reach out to us with feedback on your experience. We also have several other eBooks in our catalog that may interest you. Please review our website at allensinfosecagency.com for additional details.

https://allensinfosecagency.com/home/services/

support@allensinfosecagency.com