Cyber Security Mastery

TRAINING GUIDE

WILLIAM MCBRIDE

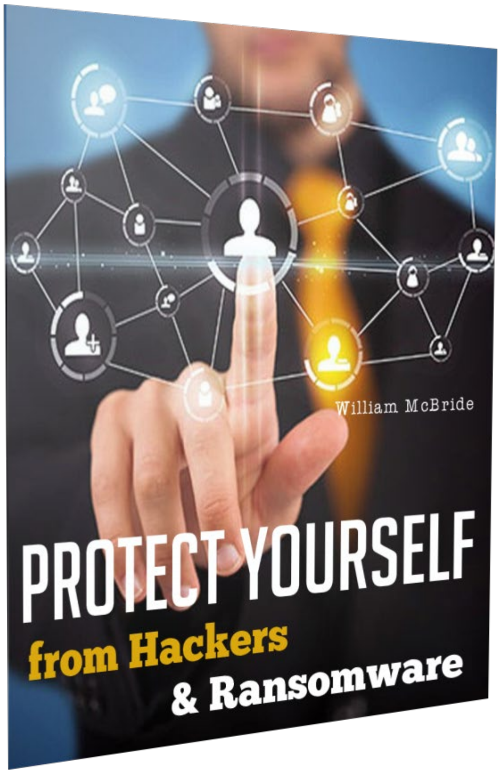
Find the Latest Information and Methods of **Cyber Security to Protect** your **Online Business**

Quality Books for Everyone

A Personal Invitation

At Quality Books for Everyone our goal is to create digital books and course that help people learn and grow.

We invite you to look at the following product and see if it might be a way to grow and expand your understanding and protect your computer data.



This is a recently released UDEMY online training video course on cyber security.

Click the red button for more details.

YES I Want This

Copyright Notice

This material is intended for education purposes only. Neither the author nor publisher provide any legal or other professional advice. If you desire professional advice, please seek advice from professional licensed individuals or companies.

This material does not provide complete information on the subject matter covered herein.

This material is intended to be used only as a general guide on the subject and is not the sole source of information on the subject(s) covered on the following pages. While the author and publisher have sought to provide careful and accurate information, there is no guarantee of accuracy or of no errors, omissions, or typographical errors. Any slights of people or organizations are unintentional.

Any reference within the material to any person or organization, living or dead is purely coincidental. The author and publisher shall have no liability or responsibility to any person or entity and hereby disclaim all liability, including liability for consequential damages regarding any claim, loss or damage that may be incurred, or alleged to have been incurred, directly or indirectly, arising out of the information provided in this material.

Furthermore, the author and publisher make no claims or guarantees of any income or monetary outcomes or reward as the result of reading and putting the educational material in this document into practice and use in one’s daily life and practice.

EBOOK DISCLAIMER

DISCLAIMER AND TERMS OF USE AGREEMENT The author and publisher have used their best efforts in preparing this eBook. The author and makes no representation or warranties with respect to the accuracy, applicability, or completeness of the contents of this book.

The information contained in this book is strictly for educational purposes only. Therefore, if you wish to apply ideas contained in this book, you are taking full responsibility for your actions and the results of your actions.

Every effort has been made to accurately represent this product and it's value to the reader. However, there is no guarantee that you will improve in any way using the techniques and ideas in these materials.

Examples in these materials are not to be interpreted as a promise or guarantee of anything. Self-help and improvement potential are entirely dependent on the person using the product, ideas and techniques explained in this book.

Your level of improvement in attaining the results claimed in these materials depends on the time you devote to the program, ideas and techniques mentioned, and your knowledge and various skills.

Since these factors differ according to individuals, situations and locations, we cannot guarantee your success or improvement level. Nor are we responsible for any of your actions.

Many factors will be important in determining your actual results and no guarantees are made that you will achieve results similar to the ones outlined in the book.

The author and publisher shall in no event be held liable to any party for any direct, indirect, punitive, special, incidental or other consequential damages arising directly or indirectly from any use of this material, which is provided “as is”, and without warranties.

As always, the advice of a competent professional should be sought.

The author and publisher do not warrant the performance, effectiveness or applicability of any sites listed or linked to in this report.

All resource links are for information purposes only and are not warranted for content, accuracy or any other implied or explicit purpose.

Promotional links are to provide additional training and products related to the topics covered in the eBook. The author may receive compensation should the reader take action and purchase any additional training or materials outlined in the product links.

Cyber Security Mastery

TRAINING GUIDE

Find the Latest Information and Methods of **Cyber Security to Protect** your **Online Business**

Table of Content

Introduction

Chapter-1 Cybersecurity – An Overview

a. Common types of threats

b. Types of cybersecurity

c. Why is it important?

d. Benefits

e. Using Automation in cyber security

f. Top cyber security challenges

Chapter-2 Latest Cyber security Trends

a. An increase in attacks on remote infrastructure

b. Smart devices will evolve from connected' to autonomous.

c. The internet will become one large, interconnected service factory.

d. More advanced, non-nation state users online will attempt to influence and disrupt.

e. Internet connectivity providers will need to provision more bandwidth excess.

f. Expect more bad bot problems.

g. Ransomware will continue to rule the land.

Chapter-3 A Guide to Hacking and how to avoid it?

a. What is hacking?

b. Types of Hackers and Hacks

c. How Hacking works

d. Why hacking is bad?

e. Tips to stay safe from hacking.

Chapter-4 How to protect your smartphone from hacking?

a. Do not Jailbreak

b. Make Smartphone Lock Sooner

c. Perform All Software Updates

d. Set up Two-Factor Authentication

e. Create Long Passcode

f. Turn On Erase Data

Chapter-5 A Guide on types of Malwares and how to handle them

a. Adware

b. Backdoors

c. Bots and Botnets

d. Browser Hijacker

e. Bug

f. Crimeware

g. Keyloggers

h. Malicious Mobile Apps

i. Phishing and Social Engineering

Chapter-6 How to guard yourself from visiting unsafe websites?

a. In-Browser Tools for Website Safety

b. Other Website Safety Tests

c. Use Trusted Retailers

d. Double Check URLs

e. Note Payment Methods

f. Check Review Sites

g. Check For HTTPS

Chapter-7 Understanding Phishing and Ransomware and how to prevent them.

a. Ransomware definition

b. How Ransomware works?

c. Who is a target for ransomware?

d. How to Prevent Ransomware Attacks?

e. Phishing definition

f. What is a phishing kit?

g. Types of phishing

h. How to prevent Phishing attacks?

Chapter-8 A Guide to creating the right cybersecurity Budget post pandemic.

a. Threat Assessment

b. Staff and Training Costs

c. Incident Response

d. Resource Replacement and Upgrade

e. Consultants

f. Insurance

Chapter-9 How should Companies adapt their new Security strategy post pandemic?

a. Adopt a Zero Trust Approach

b. Review Security Before Adding Tools

c. Make Multi-Factor Authentication Mandatory

d. Tap into Intelligent Technologies

e. Practical Security Training for the Remote Workers

Chapter-10 Case Studies

a. Case 1: A Business Trip to South America Goes South

b. Case 2: A Construction Company Gets Hammered by A Keylogger

c. Case 3: Stolen Hospital Laptop Causes Heartburn

d. Case 4: Hotel CEO Finds Unwelcome Guests in Email Account

e. Case 5: A Dark Web of Issues for A Small Government Contractor

Conclusion

Cyber Security Mastery

Introduction

The year 2020 has been a trial for most organizations, especially in the cyber security field. Despite a slowdown, companies realize the continued importance of data and systems protection, and executives are keenly aware of the role it will play in the future.

It goes without saying that the COVID year 2020 and even into 2021 has been a challenge for personal computing and protecting personal and at home data too.

While this guide speaks directly to the business computing environment, it has a strong message for you if you just do computing at home or on your smartphone.

Corporate leaders are increasingly elevating the importance of cybersecurity to their companies. Looking at the year ahead, it is critical to continue elevating cybersecurity as a strategic business issue and develop more partnerships between industries, business leaders, regulators, and policymakers.

To get started, our comprehensive and professionally researched Cyber security Training Guide will assist you at every step of creating your cyber security system this year.

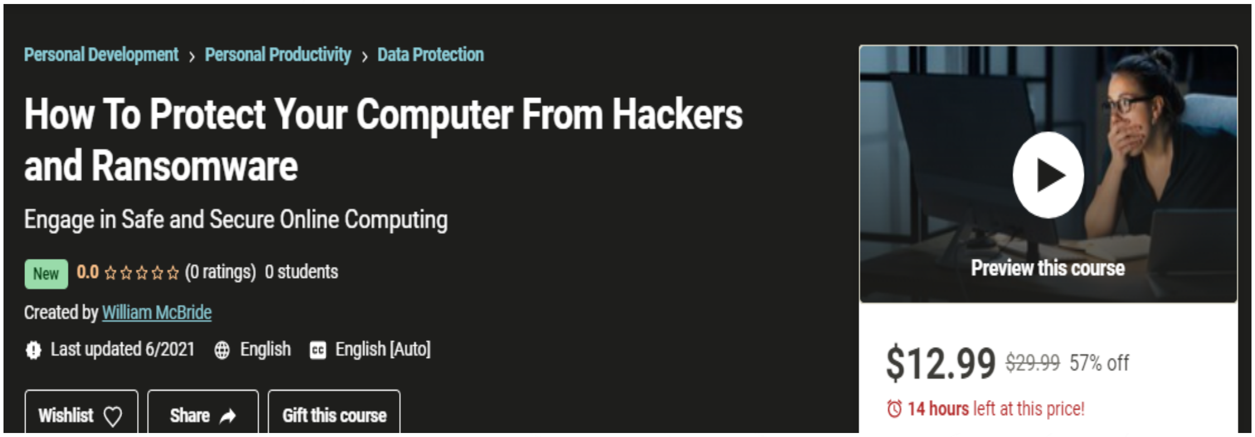
This comprehensive cybersecurity guide will help you understand all about security in the COVID era, building security plans and budgets, types of threats, how their scope is increasing and solutions to the same. Most everything in this extensive guide fits the home computing world too.

Let’s Get Started!

I’ve created a special Cyber Security online learning course published recently on the UDEMY platform.

If you’d like to check it out just click this link and watch the preview video and the free introduction to the course.

https://www.udemy.com/course/protect-yourself-from-ransomware/



Personal Development › Personal Productivity › Data Protection

How To Protect Your Computer From Hackers and Ransomware

Engage in Safe and Secure Online Computing

New 0.0 ☆☆☆☆☆ (0 ratings) 0 students

Created by William McBride

Last updated 6/2021 English English [Auto]

$12.99 ~~$29.99~~ 57% off

14 hours left at this price!

Cyber Security Mastery

CHAPTER 1

Cyber Security – An Overview

Cyber Security – Meaning

Cybersecurity is the process of protecting systems, devices, networks, and data from any type of unauthorized access or attack. Cyber-attacks typically try to gain access to sensitive information and alter, disrupt, destroy, or control that information for malicious or criminal intent.

These attacks are of increasing concern to businesses and individuals. As more information and data continues to move online, everything from emails and credit cards to navigation systems and medical records are susceptible to digital attacks.

Common Types of Threats

Cyber-attacks can vary in size and scope, but some of the common types of threats include:

- **Phishing**

This usually takes the form of emails that appear as though they are from a reputable and legitimate source. These fraudulent communications aim to steal sensitive details, such as login information or credit card numbers.

- **Malware**

Malware is malicious software that has been designed to gain unauthorized access or disrupt a computer. It typically breaches a network if a user clicks on a dangerous link, email attachment, or download. Malware can take many forms, including viruses, Trojans, worms, spyware, and ransomware.