Cybersecurity in the COVID-19 Pandemic: Protecting Your Digital Assets

The COVID-19 pandemic has had a profound impact on our lives. We have all had to adapt to new ways of working, learning, and socializing. These changes have also had a significant impact on our cybersecurity.

As we spend more time online, we are also creating more opportunities for cybercriminals to attack us. In the first half of 2020, there was a 20% increase in cyberattacks compared to the same period in 2019. This increase is expected to continue as the pandemic goes on.

Cybersecurity in the COVID-19 Pandemic by Brad Price

4.5 out of 5

Language	: English
File size	: 1508 KB
Text-to-Speech	: Enabled
Enhanced typesetting	: Enabled
Word Wise	: Enabled
Print length	: 192 pages
Screen Reader	: Supported

The types of cyberattacks that we are seeing during the pandemic are also evolving. Cybercriminals are taking advantage of the increased fear and uncertainty to launch phishing attacks, malware attacks, and ransomware attacks.

Phishing attacks are emails or text messages that appear to come from a legitimate source, but are actually designed to trick you into clicking on a malicious link or downloading a malicious file. Malware attacks are designed to infect your computer with malware, which can steal your personal information, damage your files, or even lock you out of your computer.

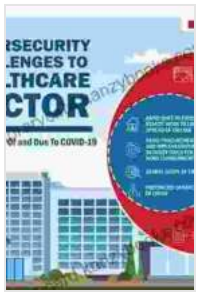
Ransomware attacks are a particularly insidious type of cyberattack. Ransomware encrypts your files, making them inaccessible. Cybercriminals then demand a ransom payment in exchange for decrypting your files.

So, what can you do to protect yourself from these cyberattacks? Here are a few tips:

- **Be wary of phishing attacks.** Do not click on links or download files from emails or text messages that you are not expecting. If you are unsure whether an email or text message is legitimate, contact the sender directly.
- **Keep your software up to date.** Software updates often include security patches that can help to protect your computer from malware attacks.
- **Use a strong password.** Your password should be at least 12 characters long and should include a mix of upper and lower case letters, numbers, and symbols.
- **Enable two-factor authentication.** Two-factor authentication requires you to enter a code from your phone or email in addition to your password when you log in to your accounts.

- **Be careful about what you share online.** Do not share your personal information, such as your Social Security number or credit card number, online unless you are sure that the website is legitimate.
- **Back up your files.** In the event of a ransomware attack, you will be able to restore your files from your backup.

By following these tips, you can help to protect yourself from cyberattacks and keep your digital assets safe.



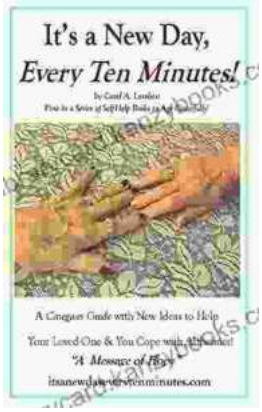
Cybersecurity in the COVID-19 Pandemic by Brad Price

4.5 out of 5

Language	: English
File size	: 1508 KB
Text-to-Speech	: Enabled
Enhanced typesetting	: Enabled
Word Wise	: Enabled
Print length	: 192 pages
Screen Reader	: Supported

Discover the Unbreakable Bond Between a Mother and Her Son in "Praying and Praising Mama"

Delve into an extraordinary narrative that celebrates the power of love, faith, and family in "Praying and Praising Mama." This captivating book will touch your...



It's a New Day Every Ten Minutes: Transform Your Life with Mindfulness

In the tapestry of life, we often get caught up in the threads of the past and the worries of the future, losing sight of the present moment. This...