Secure Electronic Payments

Staying Safe with Electronic Payments

ALLEN'S INFOSEC AGENCY

About The Author

Marwyn Allen is an Information Security enthusiast and business man. 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, Information Security firm and an events business. 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.

Staying Safe with Electronic Payments

Online, we don't get to see the person we're paying, so often it can be hard to tell whether or not your information is safe from fraud. However, sometimes it's just easier to pay online or it may be the only option available. To help ensure that you're staying safe with electronic payments, there are things you need to know and keep in mind.

1. Use Credit, Not Debit

Credit cards come with better consumer protection against fraud, and your liability is usually capped at about $50, as long as you catch the extra charges in time. Debit cards on the other hand, don't have much of a liability. Depending on when you report your card as missing, you could be held liable for the entire amount.

So, stick to credit cards. If you ever have any doubts, you can use a one-time credit card to generate a random card number to be linked to your bank account. All of this will make it harder for criminals to get hold of your money and information.

2. Check the URL

When you go onto a website that requires your private information, make sure the page's address starts with "https" and not "http". That extra "s" means that the website uses an encryption code that scrambles your information, preventing people from getting your information. The "s" doesn't always mean that the transaction is 100% safe, but it is a quick check that might be able to give you a sense of security.

You can also use online browser security tools and URL scanner tools which provides you with information on a websites reputation and threat score. Again these tools are not always 100% accurate but can be very helpful, a few of these tools are covered in my Information Security training.

3. Don’t Shop in Public

Public Wi-Fi is never secure from scammers, so buying things online with that Wi-Fi is almost begging people to take your information. Whenever you feel the need to buy things online, use private Wi-Fi and your own computer. You’ll then find that your information will be safer from lurking criminals.

4. Never Give Out Your Social Security Number

There isn’t a single reason why someone would need your social security number in order for you to buy something. If a website is asking way too many questions, leave the website and don’t make any purchases from them.

5. Use a Safe Password

Things like “12345”, your social security number, or your birthday are not strong passwords. Hackers will easily get into your private information and potentially ruin your life. If you can’t think of a secure password, use a password generator.

Do not write your passwords down anywhere. The wrong people could get their hands on that paper, so try remembering them instead. To keep your private information as safe as possible, you can also try changing your password every couple of months. This will make it that much harder for people to gain control of your information.

Your information is your information, so stay safe when shopping online because scammers are always lurking. Keep your eyes open for little clues on whether or not you’re about to be scammed. Clues will usually be hidden; you just have to know how to look for them. And if you don’t notice any clues, just trust your instincts.

If you’re on a website and you’re getting a bad feeling about what it's asking or how it looks, get off the page. It’ll be safer for you and your information.

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

By: Marwyn Allen