How to Stay Safe When Entering Your Credit Card Number on a Smartphone

TechRounder PDF Edition

Live article:
https://www.techrounder.com/technology/how-to-stay-safe-when-entering-your-credit-card-number-on-a-smartphone/

By Vipin PG | Published October 3, 2020 | Updated January 4, 2026 | Format: Guide | 3 min read

Quick answer

In essence, a modern smartphone is no different than a personal computer. You can use it for browsing the web, playing videogames, chatting with friends, and even paying your bills online.

In essence, a modern smartphone is no different than a personal computer. You can use it for browsing the web, playing videogames, chatting with friends, and even paying your bills online.

But even though you could, the question remains: should you proceed to enter your credit card number on a smartphone without a second thought, or are there traps that await? Find out more below!

Know what (and who) you're dealing with

The short answer: yes, generally speaking, it is a safe thing to do. With that being said, mindfulness is key as you do have to know who you're dealing with and recognize a potentially dangerous situation as it arises.

To give a concrete example, if you're visiting your bank's official website or paying through an official payment gateway provided by the likes of Amazon, you should be fine (as long as it's not a forgery).

If, on the other hand, someone asks you to provide your credit card details over a personal message on a forum, Facebook, eBay, or something similar, do not give in! In this example, it's almost like handing over your physical credit card to a complete stranger. Not only can you never be sure this person is who they claim to be, there is also no form of encryption used to exchange this sensitive data.

In a digital environment, it can be hard to know who's on the other side.

Learn how to recognize fraud

One of the first lessons you'll learn from cyber security experts is to never click on a link sent to you via email or personal messages whenever entering any kind of login credentials or sensitive data is involved. The reason being is that by doing so, you might fall victim to what's known as a phishing scam, which is a form of forgery and fraud.

This is how it works:

By using authoritative or convincing language and other methods of persuasion (often by pretending to be your boss, a company official, or a system administrator), a hacker will attempt to direct you to a fraudulent input form. As soon as you enter anything into it, it will get sent straight into the hacker's clutches instead of its intended destination.

Phishing can also be executed the traditional way - in this case, a hacker will call you over the phone and come up with a similar request. You may be pressured with a dire sense of urgency (which also happens to be somewhat easier to execute due to the fact that a phone conversation tends to feel more personal).

Ensure that no one can intercept the data you send

The data you send online can only be as safe as your connection allows for. In other words, be mindful when accessing the internet through Wi-Fi a coffee shop will typically offer their customers. Since anyone can connect to it, even an amateur hacker could be eavesdropping on your data.

Additionally, any website you make payments on should use the secure HTTPS protocol and display certificates of trustworthiness. This is true for every country or region. For example, take a look at this online roulette in India and scroll down to the footer section of the website. You'll see a myriad of certificates and licenses that are renewed on a daily basis to instill customer trust. And in the upper portion of your browser, you'll see a lock icon, indicating that the website uses encryption.

Extra tip: use a dedicated card for online purchases

To conclude this train of thoughts, we'll share one last nugget of wisdom for today: if you're extra paranoid, you can also use a separate card for online purchases. This can be either a virtual card or a card issued by your bank separately. The idea is to not keep all of your funds on it, but only a fraction - the kind you'd need to make an online purchase (or just fill it up on demand). That way, even if someone were to steal your credit card info somehow, there'd be nothing on it to steal.

Conclusion

As long as you keep everything we've said in mind, you should be more than confident in entering your credit card details on a smartphone. Believe it or not, common sense goes a long way; it's the best security measure of all.

References

1. security.berkeley.edu - education-awareness / phishing - https://security.berkeley.edu/education-awareness/phishing/phishing-examples-archive

2. experian.com - blogs / ask-experian - https://www.experian.com/blogs/ask-experian/what-is-a-virtual-credit-card/