Giesecke+Devrient

Trend report

Securing everyday digital payments: How secure are your online payments?

Ok, we are getting tired of hearing about Covid-19, and we all know the drill with lock downs, social distancing and all. Now we just want to focus on getting back to some sort of normal, even though that normal most probably will look very differently as we know it. One big change throughout 2020, that most probably will stay, is how e-commerce has been booming. And still is. Digitally savvy online shoppers have easily moved from physical stores to online, not only for shopping shoes and clothes or streaming film and music. But also, to order food, gardening utilities and beyond. But how secure is it to shop and pay online?

Forrester researchers predicted that online retail would grow 18.5% in North America in 2020, reaching 20.2% overall penetration. And when looking back at the Christmas season, we noticed it was not only the usual online shoppers ramping up their game. We also saw a strong demographic shift, with the Boomers going online to buy and send gifts for the Holidays. As online buyer behavior will continue to strongly increase, online merchants need to adapt rapidly to cater the customers, and getting the payment offering right is crucial in order to offer a safe and secure online shopping experience. Cause fact is this new customer group will be an easy target for fraud and scams. And here the payment ecosystem needs to step up and educate about the risks when it comes to online shopping!

e-commerce in times of Covid-19

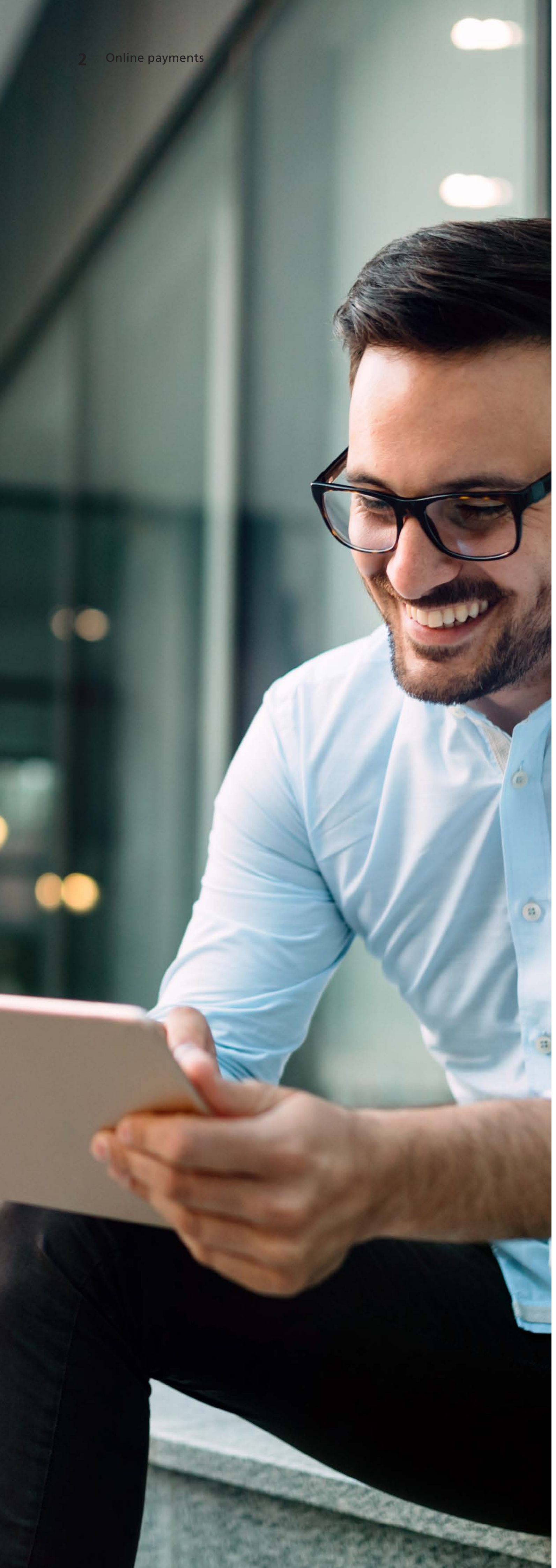
The pandemic has driven retail online, to fulfill social distancing requirements. 48% more US consumers used digital channels to shop during the first months of the crisis than before.

1/5 of consumers in Asia Pacific went online for the first time.

E-commerce sites have undergone an unprecedented global traffic increase, surpassing even Holiday season traffic peaks. Overall, they have generated almost 22 billion visits (June 2020), up from 16.07 billion global visits (January 2020).

A survey conducted by Dynata for Redpoint Global, found nearly two-thirds of the adult shoppers surveyed planned to do all their Holiday shopping online.

(Sources: G+D Market Intel, BCG, Accenture, Statista)



As a solution to secure the online shoppers, and still getting the conversions at the checkout, **Jukka Yliuntinen, Head of Digital Payment Solutions at Giesecke+Devrient (G+D), strongly promotes Card-on-File (CoF) network tokenization of payment card credentials.**

"In major geographies, overall consumer payments revenue is largely driven by spending-dependent streams, especially cards. These streams account for between 66 % and 86 % share, with the rest driven by liquidity and account-based revenue", Jukka says. "Some spending is expected to move to e-commerce where possible, but less developed e-commerce sectors will be hit significantly – some by more than 50 %, initial data suggests. Securing these transactions not only delivers increased revenue. **With CoF network tokenization you will also eliminate risk and serve your customers with a happy shopping experience.**

The rise of tokenized digital payments is also something we at G+D notice when looking at own statistics: "Our numbers not only confirm this trend, but also are proofing an even higher impact based on the increase of customers going digital, as this is hitting all-time-high records in an accelerated pace!", Jukka says.

But how can a customer have control over who has access to this payments data? What if someone gets hold of card numbers and CVV codes, and misuses the information? Recent reports show that phishing scams are on the rise, targeting consumers primarily through email, secondarily through text messages but also thru reach out via direct phone calls. Actually, as many as 27% of consumers have been hit with pandemic-themed phishing scams, according to a survey done by TransUnion.

How to avoid phishing scams and fake web shops

- If receiving an e-mail, make sure to check out the sender. If you are unsure or if something feels strange, if there is a lot of spelling mistakes or attachments to open, assume the e-mail is fraudulent and remove it immediately.
- Don't open attachments and don't click on links from unknown senders.
- If you get contacted via phone or direct messages on social media or such, apply the same as for an e-mail.
- And never ever hand put your card details, codes, passwords to a third party!
- To see if an online shop is fake, click on the imprint for legal information. If this is missing out, the shop is a no go.
- Google the web shop's name and look for reviews. Or even check-up the shop on Trustpilot and alike to learn more about the online shop.
- Does the shop have certificates, proofing it is trustworthy? Click on the logos: If the certificates are real, they also link to the certifying organization for further information.
- When it comes to pay, look at the checkout and validate how the payment is processed. If done via renowned payment network providers, the checkout process is most likely secured. But if suddenly you should send your card details via e-mail, or fill out a form, or pre-pay in any way, abandon the process as this might be a fraud.
- And finally, use your common sense: If it is too cheap, too easy, too many logos, too many misspelled words, it is probably too good to be true.

(Sources: G+D Market Intel)

One attempt to prevent online scams is made from the EU commission, who has met and urged online merchant platforms to join forces with consumer protection authorities on tackling online consumer scams. Which are good initiatives for sure. But there are ways to include the card holders too, and let the consumer take ownership of its payment credentials.

Jukka explains how this is done: "With our latest innovation, our Token Cockpit, we provide the end-customer a token management tool integrated for example in the mobile banking app, fully controlled by the end-customer itself. In this cockpit, the customer has a full overview of where the payment credentials are tokenized, and can also enable and revoke tokenized cards, for total control. This empowers end-user to deploy the mobile phone as a remote controller of payment cards for all digital channels. Then the Cockpit provides same enablers to Issuing banks in terms of web-UI, for customer support purposes."

But at the end of the day, when it comes to pay securely online, the whole ecosystem consisting of payment service providers, online merchants, card networks, issuers and the consumers themselves need to **take control to prevail over the fraudsters.**

"To gain success in this increasingly complex arena, online merchants for instance will need to work with the right partners. G+D offers end-to-end solutions for e-commerce and tokenized payments, enabling security with CoF network tokenization and a state-of-the-art customer experience for increased conversion rates." Jukka continues: "For banks to offer a complete security solution, allowing the customers to have a transparent and fully control of their payments data, the Token Cockpit is a sophisticated way to bypass fraudsters in getting hold of and misuse card details: The customer can easily monitor where the tokenized credentials are afoot, and in a jiffy revoke or momentarily disable the same if wanted. Banks eliminate the risks of costly security breaches, the customers feel confident in how their payments are in use, and the customer relationship is strengthened. And the right merchants receive payments at the checkout. **A win-win for everyone!"**

About Giesecke+Devrient

Giesecke+Devrient (G+D) is an international Group providing security technology and headquartered in Munich, Germany. Innovations by G+D make the lives of billions of people in the digital and physical world more secure. With its products and solutions, G+D is one of the market and technology leaders in payments, connectivity, identities, and digital infrastructures.

Established in 1852, the company achieved sales of €2.45 billion in the fiscal year 2019 and employs 11,500 people. G+D has a presence in 33 countries. Its customer base includes central and commercial banks, mobile network providers, automotive manufacturers, health insurance companies, and governments and public authorities. Further information: www.gi-de.com.

Giesecke+Devrient

Giesecke+Devrient Mobile Security GmbH
Prinzregentenstrasse 159
81677 Munich
Germany

www.gi-de.com
mobilesecurity@gi-de.com

Follow us on: