NuData Security
mastercard

Shoppers are going digital, but is your user experience keeping up?

MERCHANT EBOOK

EBOOK

Improving your user's experience with behavioral biometrics. Take this crisis as an opportunity to create a better user experience with behavioral technologies.

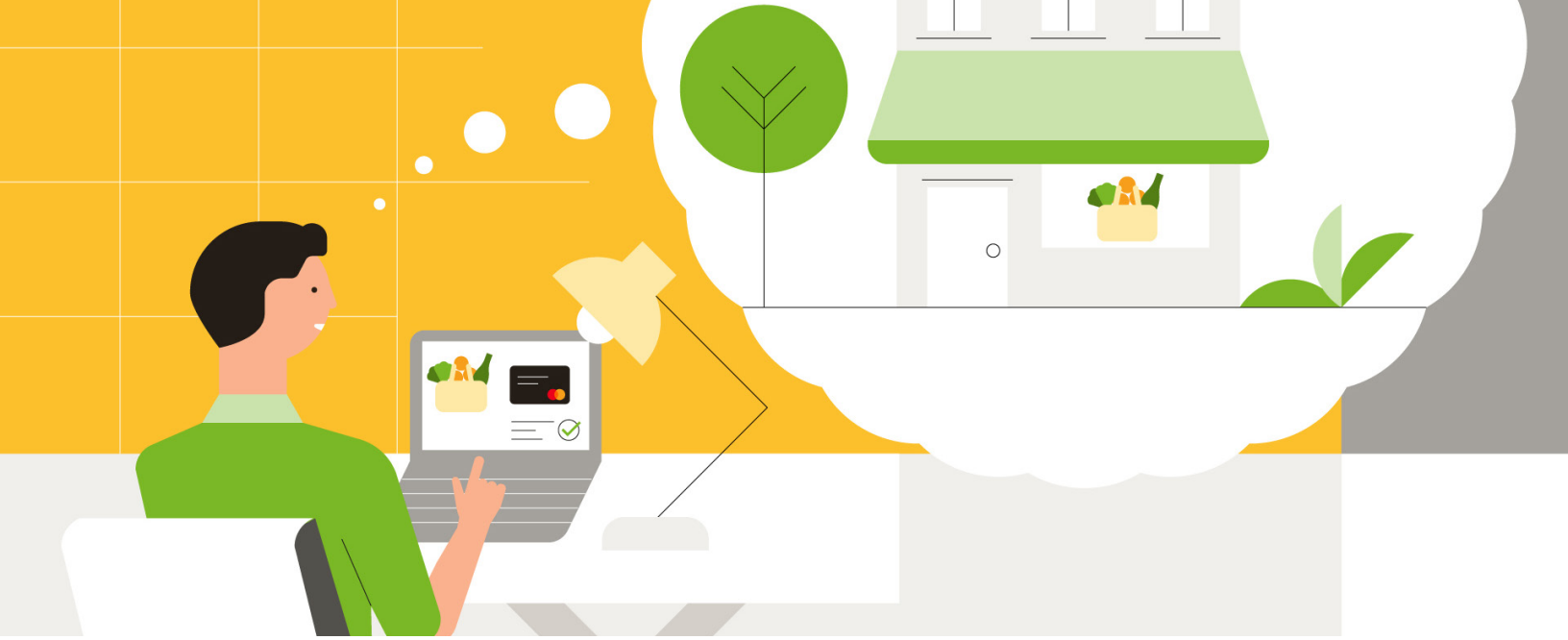
The temporary closure of brick and mortar storefronts is driving buyers to online marketplaces. Digital goods companies, although unaffected by physical closures, are also benefiting from the public's new hunger for online entertainment – whether that is watching movies, playing online games, or using apps to talk to friends and family.

If you are a merchant offering your services online, you have probably seen an increase in users and new account creation in the last several weeks. Although this is good news, many of them are not your traditional online users.

A portion of this new customer base prefers physical stores but are now forced to access goods online. These customers, often not very computer-savvy, demand seamless online experiences to help them adapt to the new way of life.

Impacted businesses are at a crossroads: they can keep their online customer experience as it is or adapt it to help new customers during this transition. Once movement restrictions are over and people hit the streets again, customers who favor brick and mortar storefronts could leave the online space just as quickly.

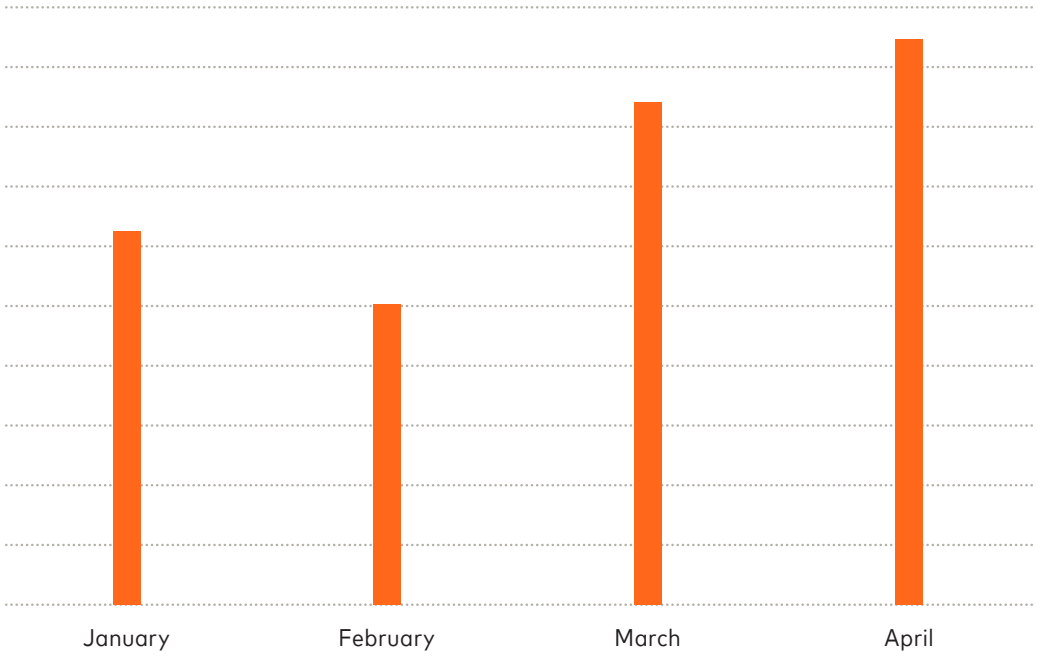
Yet, merchants that make extra efforts to improve the digital user experience without compromising security will increase their chances of keeping these new customers for the long term. Technologies that look at the user's online behavior like behavioral analytics and passive biometrics help remove friction to simplify the customer journey. If there is a time when stepping up your security measures and giving your customers a better experience is vital, this is it.



Shoppers going digital

The presence of new users in the online space is palpable in the NuData network, where we see that the creation of new eCommerce accounts has increased by 62% in March of 2020, when most lockdowns and restrictions came into play – compared to January and February. April is following the same upward trend.

Volume changes of new accounts



Global New account traffic volume from eCommerce companies. Source: NuData

Global retail company traffic

Global retail company traffic from October of 2019 to April of 2020. Source: NuData

The challenges of balancing user experience and security

Cybercriminals are taking advantage of the virus to carry out COVID-related phishing campaigns, malware via malicious links and attachments, ransomware attacks, or eCommerce scams. These attacks are filling up bad actors' Excel sheets with new username and password combinations. Every day, fraudsters are probing online websites and apps to find any security gap to deploy attacks such as credential stuffing or make fraudulent purchases.

At the same time, with more customers shopping from home and unable to commute or travel, legitimate user behavior is changing. For example, if a user looks like they have traveled to another country when they log in, now there is a higher probability that it is fraudulent. Similarly,

with so many new users behaving differently, such as logging in at unexpected times of the day, static risk management tools are likely to falsely decline many legitimate money transfer attempts.

This combination of bad actors using fresh credentials and users behaving differently can lead companies to mistakenly assess their customer's legitimacy. Failure to accurately verify a user can increase false declines or unwillingly allow fraudulent actors into an account.

On the other hand, to avoid good users from being blocked and complete the transaction, some companies are tempted to remove security barriers, such as one-time password requests. Although this would improve the customer experience, it increases the chances of fraud.

Reducing user friction can only be done safely if there are other transparent technologies in place that detect human-driven and automated attacks, such as behavioral analytics and passive biometrics. These technologies help evaluate any activity without impacting the user experience.

44%

of consumers stopped shopping at a retailer as a result of false declines[1]

$443B

is the estimated cost of false declines by 2021[2]

[1] Javelin Advisory Services, *Addressing the Threat of False Positive Declines*, 2018.
[2] Aite, *The Ecommerce Conundrum*, 2019.

Leveraging behavioral technology to retain new and existing customers

Behavioral and passive biometrics technologies have the benefit of identifying suspicious activity and recognizing trusted users without relying on credentials or personally identifiable information. These technologies create a seamless experience for new and existing users.

How behavioral analytics and passive biometrics work

The combination of these two technologies can verify a user based on how they behave in the environment. Information such as how someone types, holds the device, and hundreds of other data points, builds an accurate online profile. This real-time assessment helps decide if there is a machine or a human behind the device. And, if it is a human, passive biometrics also determine if it is the legitimate owner of the account or an impostor trying to take over someone's account. For example, if a customer changes devices and logs in from a new computer, their typing pattern and other inherent parameters can determine, without additional friction, if it is the same legitimate user or not.

Adding machine learning to adapt to changing behaviors

Passive biometrics and behavioral technologies gather hundreds of anonymized data points from every user interaction. That data is fed into a machine learning tool in real time to detect subtle changes in traffic patterns and adapt to them.

According to NuData analysts, customers interact with an average of three devices (work computer, home computer, and mobile device) from different locations that security models can recognize as frequent and safe, removing unnecessary friction.

WHAT ARE BEHAVIORAL ANALYTICS AND PASSIVE BIOMETRICS?

Behavioral analytics is a technology that evaluates signals across the user interaction. Looking at the device, type of browser, type of information input, and other parameters help determine if the user is behaving like a good user or like a bad actor.

Passive biometrics builds an online user profile based on a user's inherent behavior when they interact with a device. The typing cadence, how one holds the device, and other parameters build a unique profile. This technology determines if the behavior from a user matches the behavior of that same user in the past. This effectively determines not only if the behavior is that of a good user, but if it is indeed the expected behavior of this user.

This real-time evolution of the machine learning models helps merchants recognize their trusted users and remove verification step-ups, such as one-time passwords, security questions, or the CVC number on their credit card at checkout.

Applying intelligent interdiction

Seamless security doesn't mean removing all friction permanently, but rather using friction intelligently. A trusted user shouldn't need to prove their identity at every interaction during a purchase; only users showing risky traits should be presented with added verification steps. These can be a physical biometric request, a one-time password, or a CAPTCHA challenge, among others.

To improve the entire customer journey, behavioral technology can be placed at any point, including account creation, login, or checkout. This allows end-to-end monitoring of a purchase to reduce friction at every step.

Benefits of a behavioral security approach – How a Fortune 200 eCommerce company makes shopping simpler

A large eCommerce company that was the target of large cyber-attacks wanted to improve their user experience, but feared that removing friction could invite more fraud attacks to their platform.

After implementing a behavioral and passive biometrics verification solution for login and checkout, they were able to reduce friction on most of their users while keeping attacks at bay.

Results with behavioral and passive biometrics verification

- 70% of the company's trusted users benefit from reduced friction across their journey
- The security tool has mitigated attacks with 99.9% accuracy

In conclusion

Evaluating users with real-time behavioral and passive biometrics technologies – rather than relying on static usernames and passwords – helps companies verify customers without added friction. This approach to user verification simplifies and improves the experience of buyers who depend on the internet to get their goods and services. It helps brands build trust with their new and existing users and strengthen relationships.

At the same time, it allows companies to use step-up tools—which can confuse or impact the user's experience—for high-risk traffic only and reduce false declines.

Read more client stories **here**

To learn more about how to improve your user's verification experience contact verifygoodusers@nudatasecurity.com

ABOUT NUDATA

NuData Security is a Mastercard company that helps businesses identify users based on their online interactions and stops all forms of automated fraud. By analyzing over 650 billion events only in 2019, NuData harnesses the power of behavioral and biometric analysis, enabling its clients to identify the human behind the device accurately without additional friction. This allows clients to verify users before a critical decision, reduce customer insult, block account takeover, and stop automated attacks. NuData's solutions are used by some of the biggest brands in the world to offer a great customer experience while preventing fraud.

NuData Security
mastercard