Luxury Daily®

The News and Intelligence You Need on Luxury

COLUMNS

Dangers of password-based loyalty programs

June 27, 2018

George Avetisov is CEO of HYPR

By George Avetisov

Retailers work hard to deliver a memorable customer experience, so much so that shopping is now both recreation and a necessity.

Loyalty programs are key to customer retention, as customers expect a vibrant rewards system to accompany a retailer's main product offerings.

With expectations high and some standout loyalty points available, negative news about loyalty programs gains notice.

Loyalty fraud, a kind of credentials-based fraud, curbs our optimism about shopping.

Point taken

Attacks on loyalty programs are on the rise and it is concerning to retailers since they bear the costs of fraud in the form of lost dollars and trust.

Restitution for loyalty fraud is complex and touchy.

A grey area, rewards points bear a similar value to cash, yet they are not true currency.

Rewards are retailers' promise to offer the best experience, and to come full circle retailers will design the best loyalty programs and make restitution when they are breached.

Consumers sometimes build war chests of loyalty points before redeeming them, and often these reserves go unnoticed.

Loyalty accounts go unused or unmonitored by at least 44 percent of shoppers. Still, they are big business for consumers, retailers and hackers.

With 3.8 billion loyalty memberships nationwide, and stolen retail rewards selling between $2 to $10 per account on the dark Web, loyalty programs are a lucrative source for fraudsters.

If we are going to eliminate the cause of loyalty and other fraud affecting retail, we will need to rethink the technology that serves as the place where retailers and consumers exchange value.

Cred alert

We should first consider that loyalty points are stolen from the central repositories that hold and protect them. This is the same as access credentials: biometrics, PINs, passwords and bankcards.

The core vulnerability in most access systems is where this data is stored.

When loyalty points are stored centrally alongside credit card data, it creates a juicy target for those who carry out credential reuse attacks.

Retailers appreciate that a wholesale model is preferable to a retail one, and hackers live nicely on similar slim margins. It stems from the ubiquity access credentials, the failure of ways to manage them, and the fact that some credentials are used by anyone who holds them.

Credential reuse attacks arise from passwords, whose hassles inspire people to use the same username and password across different services.

Hackers obtain credentials from a prior breach, for instance, at a social media platform, and conduct automated spray-and-pray attacks at banks and retailers.

Credential reuse attacks have a 2 percent success rate, which seems meager until you consider that 3 billion breached credentials are out in the wild.

Right now, unaccounted-for credentials are being slammed against retailer servers, and those that are matched release all kinds of goodies including loyalty points.

In this context a retailer with a strong, confident security provider is no more secure than one with a weak one.

Attacks on one large online service provider are everyone's problem and will be until we invert the model that is exploited for these attacks.

The way to do that fully and efficiently without displacing other systems is to decentralize authentication data used for login, purchases and account management.

On the heels of Mastercard, some retailers are decentralizing access credentials such as biometrics, PINs, passwords and bankcards, isolating and encrypting them on everyday mobile devices that consumers already carry. This minimizes the risk of a mass data breach, removes hackers' favorite target, the credential store that is the No. 1 cause of data breaches.

Verizon reports that 81 percent of data breaches are credentials-based, so there is urgency around solutions to manage credentials differently and properly.

Pass the word

Giving consumers the power to manage data once deemed private hearkens back to when people held their valuables in a wallet and presented them only at the time of service.

Now, a person's smartphone serves as a secure digital wallet and key into applications on that device as well as on other platforms and channels.

Smartphones are capable of all kinds of password-less experiences including biometrics, helping consumers and enterprises phase out passwords.

There are many arguments against the use of passwords. They offer poor security since they are easily transferable, are linked to shopping cart abandonment, and even when decentralized they rank lower on experience vis-a-vis password-less experience.

Password-less experiences secured with decentralization are also proven to increase transaction speeds by up to 200 percent.

Decentralizing credentials is a sure way to end credential reuse attacks and the resulting payment and loyalty fraud.

As we work to decease the security incidents plaguing large enterprises that hold valuable data, and their customers, some will still take a conservative view on how to do this.

Those with a more conventional approach can look at open standards for decentralized authentication and password elimination such as those developed by the Fast IDentity Online (FIDO) Alliance, an industry consortium of our economy's best and brightest.

AN IMPORTANT DISTINCTION between password-less experiences and a true password-less architecture such as FIDO authentication is that the latter kills the password entirely, along with associated costs and challenges. The former are technologies that mask or backburner the use of passwords, which upon closer inspection reveals that a centralized credential store still exists.

Only when we migrate to systems that are genuinely free of passwords, will we end credentials-based fraud that affects everything from the bottom line to hard-earned brand loyalty.

George Avetisov is CEO of HYPR, New York.