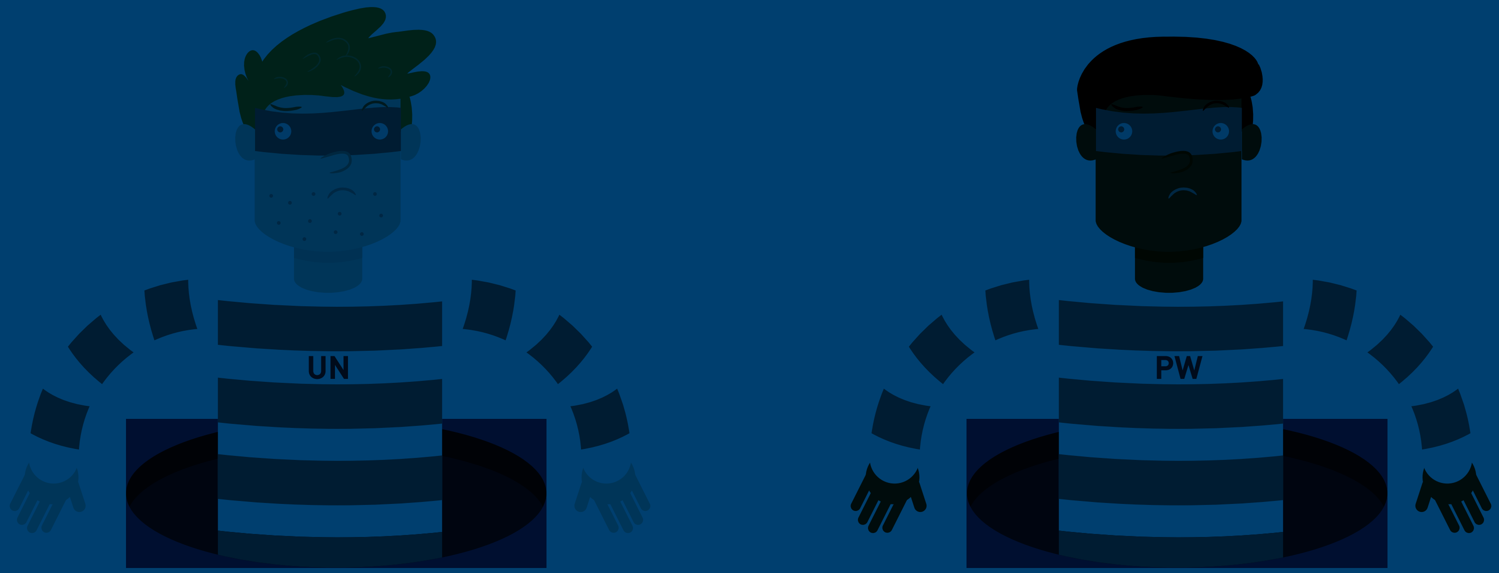
USERNAMES & PASSWORDS:

The real bandits of your e-commerce business



wwpass®

WHY YOUR E-COMMERCE BUSINESS IS LOSING SALES – AND WHAT TO DO ABOUT IT

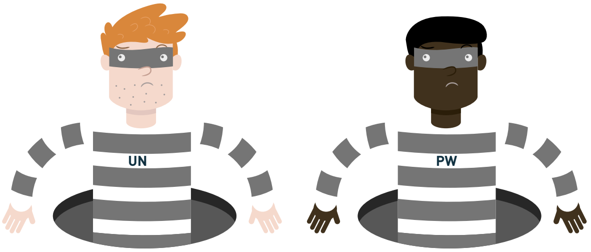
Imagine waking up to find out your e-commerce business suffered a breach – and there was something you could have done to prevent it.

What a nightmare.

You worked hard to build your e-commerce business and website. You're providing customers with an enjoyable shopping experience – from welcome to purchase to loyalty – to keep them happy and coming back for more. But, do you have the proper protocols in place to ensure you're protecting customers from fraud?

Turns out, there are two bandits you probably don't even know about that are robbing you of at least half your sales.

They are: Usernames and Passwords .

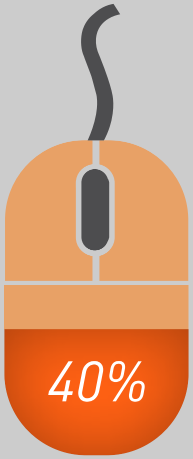


The online shopping industry is booming, and it's only going to increase – making your business a goldmine for cyber criminals everywhere.

The big question: With more and more transactions completed online, how do you protect your e-commerce site from being hacked and your customers' data from being stolen?

This guide will provide insight on how traditional authentication processes rob your e-commerce business. We'll give you the information you need to protect your business from tomorrow's breach.

*About **40 percent of internet users** in the U.S. stated they purchase items online several times per month.*



SAYING GOODBYE TO USERNAMES & PASSWORDS

Username and password combinations are known as human-readable credentials (HRC), and they're the biggest lapse in internet security.

LET'S GET DOWN TO BUSINESS...

The results have been predictable for years: people don't pick very secure passwords.

Perhaps the most overlooked element of compliance is logging in. Whether it's an administrator or a customer, simple password-based credentials alone aren't enough to secure such valuable data like customers' addresses, phone numbers, credit cards and more.

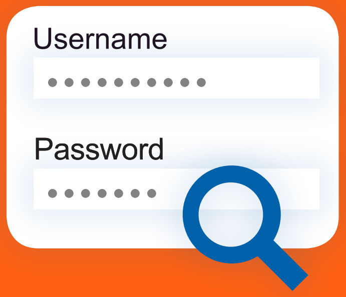
At the 2017 Blackhat Cybersecurity conference, Facebook CISO Alex Stamos reported that passwords are the biggest security challenge Facebook faces.

Spoiler alert: Passwords are not secure. Nor are they convenient.

Each of us have our own reasons for despising them. It's no longer a question of how many catastrophes it will take for people to learn – they've been dominating headlines. Rather, it's a question of when we'll see widespread adoption of a secure and convenient replacement.

This isn't a problem with an easy solution; it's a structural weakness, which requires rebuilding and changing habits. Major network authorities such as the Department of Commerce's National Institute of Standards and Technology (NIST) are already planning to restructure access control to evaluate the administration, enforcement, performance and support properties of all access control systems, such as customers logging into your e-commerce website.

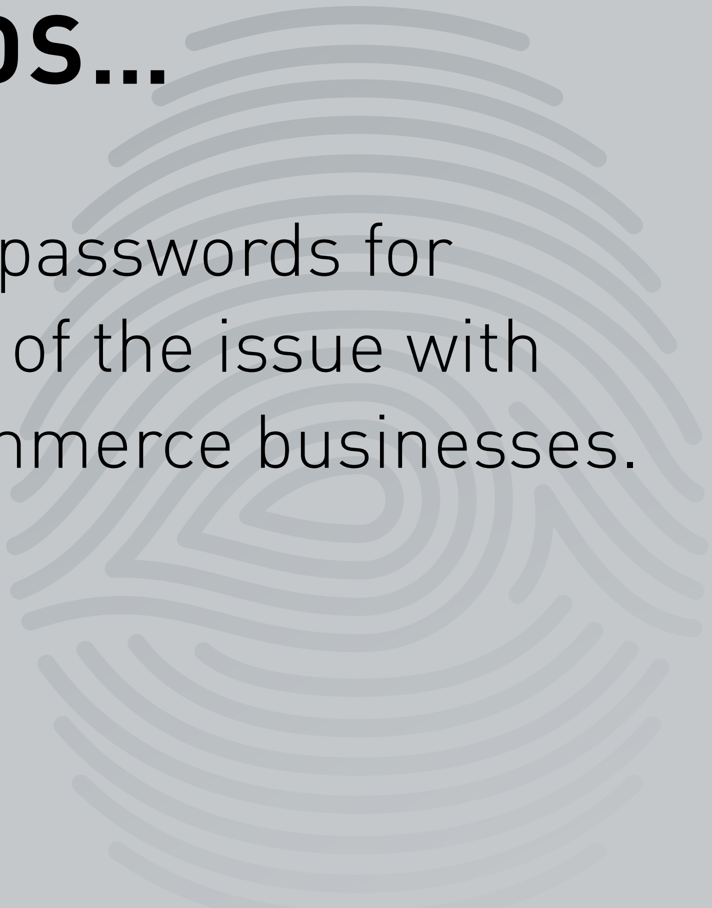
About 81 percent of security breaches are from stolen usernames and passwords, according to Verizon's Data Breach Investigations Report.

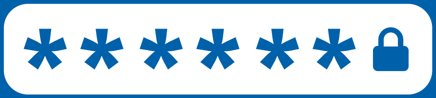


81%

GOING BEYOND USERNAMES & PASSWORDS...

The use of usernames and passwords for authentication is just one part of the issue with proper security hygiene for e-commerce businesses.





I'M PCI DSS-COMPLIANT. IS THAT ENOUGH?

Nope.

Compliance does not equal security.

The newest Payment Card Industry Data Security Standard (PCI DSS), which was released in February 2018, provides a good start for basic security measures necessary to reduce security breach risks. Unfortunately, it's not sufficient to keep customers' data secure.

We saw this with the Target, Kmart, eBay and recent Saks' Fifth Avenue incidents. All companies passed the PCI DSS audit. In fact, Target was a security standout when it passed its PCI DSS audit back in 2013, but its compliance only protected the company from liability. It did not protect it from loss of data, loss of business or damaged reputation. These breaches happened because of the use of usernames and passwords, as well as other insufficient cybersecurity protocols. The only PCI DSS requirement for passwords is that they must:

- Be at least seven characters;
- Contain both numeric and alphabetic characters; and
- Require users to create new ones at least every 90 days.

The PCI DSS rules are based on best practices and analysis of past security breaches in longstanding environments. But this is not adequate to safeguard against future breaches.

BEING SECURE TODAY DOESN'T MEAN BEING SECURE TOMORROW.

A company is only as strong as its weakest link.

PCI DSS compliancy is a requirement, but in order to decrease vulnerabilities in your e-commerce website, it's essential to perform regular PCI scans about once a quarter. Compliance is a minimal deterrent and a snapshot of how your security program meets a standard set of security requirements. It should not give companies assurance that they are "breach-proof" and their customers' data is safe.

As we learned with the Target, Neiman Marcus and Saks' Fifth Avenue breaches, the IT landscape changes so rapidly, new security measures beyond the PCI DSS requirements are necessary.

It's up to you to keep yourself accountable and complete these scans to stay ahead of cyber criminals.

TARGET®

Neiman Marcus

Saks Fifth Avenue

PROTECT AGAINST HACKERS' TRICKS: PSYCHOLOGICAL MANIPULATION AND PASSWORD THEFT

The top three types of hacks that target the e-commerce industry and involve the use of usernames and passwords include:

1 MAN IN THE MIDDLE

Rogue interception of HRC through scam or identity theft

Whether hackers impersonate a user or a company rep, a well-run scam will work on someone eventually. Social engineering and various schemes can intercept emails and text messages, extracting credentials through the communication.

2 PHISHING

A hacker's attempt to disguise themselves as a trustworthy entity, tricking users into giving up information

Common email schemes that broadly target company accounts in attempts to disrupt the network or steal valuable data work, too. Phishing emails have an open rate of 30 percent, according to the 2016 Verizon Data Breach Investigations Report. Stolen user credentials are just one part of phishing. It remains the most successful delivery method of network-crippling malware.

3 BRUTE FORCE

Unauthorized intrusion through systematic trial-and-error

Guessing will eventually work: Passwords such as "123456" and "password" barely require snooping, and programs called "password crackers" systematically try all possibilities. Both styles of intrusion are why weak passphrases have got to go. A simple password can be cracked in minutes, while a complicated one can take years. Also, password-guessing software isn't regulated. Many are open source and free to download.

HERE'S THE DILEMMA:

If you want to implement additional security measures — which may increase protection of customers' data and reduce fraudulent transactions — you could lose customers if it takes them longer to complete transactions.

Many e-commerce businesses adopt processes called two-factor authentication (2FA) or multi-factor authentication (MFA), which are intended as an extra layer of security beyond the traditional username and password.

However, customers shop online for the convenience. Your shopping and checkout process also needs to be easy, and traditional 2FA, such as SMS texts, may significantly reduce usability of e-commerce websites, which creates frustration for even the most loyal customers. Additionally, the SMS verification code could end up being sent directly to a hacker, defeating the purpose of the extra security layer.

MFA AND CYBER-DEFENSE OPTIONS:

Security Questions	*SMS or Email Confirmation Codes*	*Biometrics*	*Software Authentication Keys*
With verification questions, it's ill-advised to give valuable and unchangeable personal information associated with the user's account. There are too many digital footprints and clues that lead intruders right into people's accounts. The "secret" answers are stolen the same way they steal passwords.	While our phones and emails seem secure, they are the most common cyber attack vectors. Hackers can intercept confirmation codes via SMS with the same illegal password interception strategy. Many businesses are abandoning this method because it's functionally two easily-swindled passwords instead of one.	Getting there, but still not foolproof. There are many ways to recreate biometrics and fool the authentication. Commercial scanners for use with personal devices are just converted into readable and steal-able data, just like the password.	Encrypted security keys like smart cards or USB sticks are effective, if they don't get lost (an unavoidable human error risk). This option might be more difficult for widespread use, but it solves the problem of HRCs by getting rid of them completely.
Cyber-Defense Rating: ★☆☆☆☆	*Cyber-Defense Rating:* ★★☆☆☆	*Cyber-Defense Rating:* ★★★☆☆	*Cyber-Defense Rating:* ★★★★★

Despite multiple authentication methods backing up passwords, they still don't address the fundamental problem: All human input is vulnerable. At the end of the day, increases in security protocols do not need to be associated with decreases in usability unless one sticks to old-fashioned, obsolete approaches.

LOCKING THESE BANDITS UP (THE RIGHT WAY) ...

For the best security, don't rely on one "best" factor — implement right-factor authentication combinations.

A password isn't restricted by any proprietary information—anyone can know or guess one. So, as a means of proving identity, a password doesn't do much, and it can expose your e-commerce business to attacks. Effective security makes use of three different form factors for authentication.

A company is only as strong as its weakest link.

Something you know *(password)*

Something you have *(token)*

Something you are *(biometric information)*

However, there's still the issue of implementing these effectively without turning away customers due to a poor user experience.

While it's easier to calculate the damage from fraudulent transactions, revenue losses from potential user drop off or incomplete transactions are much harder to calculate. The latter can have a massive impact on companies.

JOIN THE PASSWORD-LESS REVOLUTION AND USE THE RIGHT AUTHENTICATION.

If it’s online, it’s a risk.

The best authentication approach is one that eliminates the weakest link in most authentication models: the username and password pairs that can be easily hacked and phished. Instead of having your customers prove their identity with a username, they should prove it with their personal pass key or token.

A different approach to authentication may be inevitable, as well. A devastating cyberattack and revised compliance regulations may cause enough of a stir to expedite a major change to internet standards.

What you need: *A single secure electronic identity that allows access to many websites, applications and other systems.*

It’s easy to combine with biometrics and PINs if you require additional verification factors, and users can revoke and securely restore lost credentials.

HOW IT WORKS:

1. Your website or app generates a QR code for authentication instead of using a social login, username or password field.

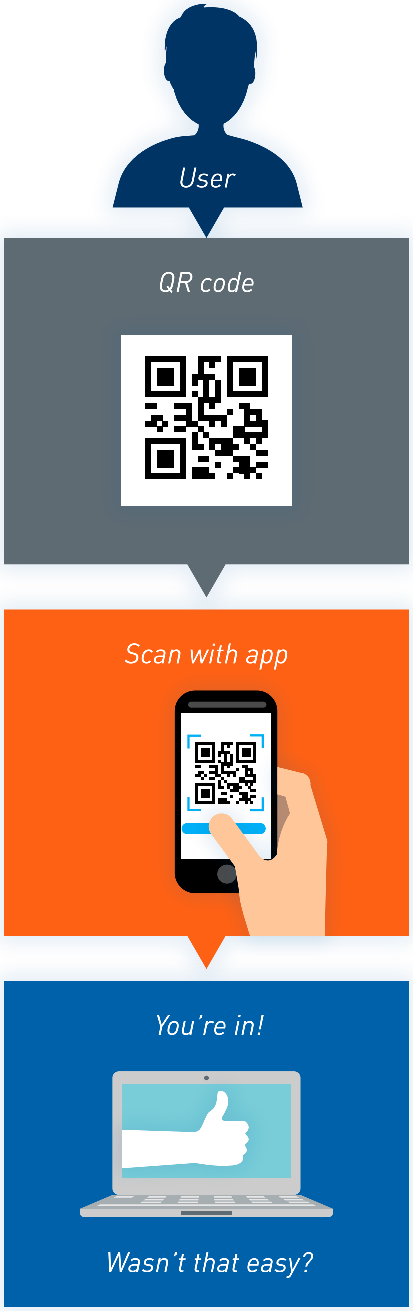
2. Your customer downloads an app on his or her phone (which acts as a unique electronic ID) to scan the QR code.

3. Customers log in to your app or website by scanning the QR code with their app.

The whole process is fast, easy and secure without usernames or passwords. If your customers need to reset their passwords, they may change their minds about a purchase by the time they access their accounts again. According to User Interface Engineering (UIE) research, customer purchases increased 45 percent when they didn't have to create a new username and password login.

Don't let your business become a statistic. Evaluate your e-commerce business' security hygiene today.

It's not a matter of if you'll suffer a breach; it's when.

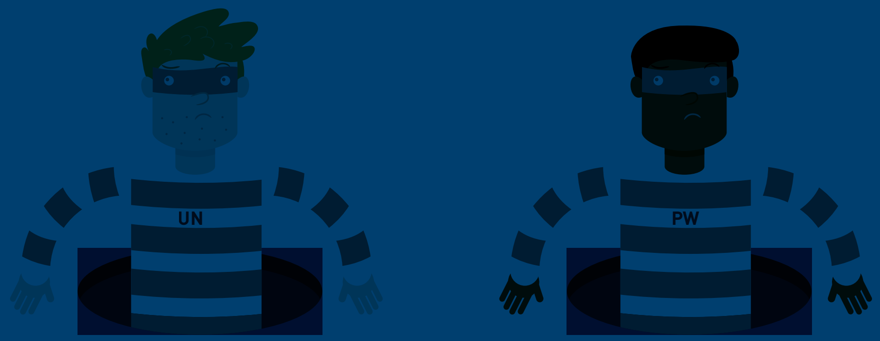


Ready to protect your e-commerce business and customers?

Contact us today.

Know an e-commerce business using dangerous logins?

Share this to get the word out:



wwpass®