The Passwordless Future

ARCULUS

The Passwordless Future

What does it look like and how do we get there?

Passwords are ubiquitous in the digital age, but they remain vulnerable to malicious attacks that can result in significant financial losses for companies. Poor password hygiene, phishing scams, and the reuse of passwords across multiple accounts have made it easier for hackers to gain access to sensitive information, rendering many popular forms of two-factor authentication insufficient as hackers use sophisticated malware to hijack authentication tools.

Increasingly, the world is moving toward passwordless methods of authentication, leveraging multi-factor authentication tools that use public key cryptography like FIDO2. Businesses that get on board will be able to leverage technologies–like Arculus Business Solutions–that combine enhanced security with an extremely user-friendly experience. Arculus Business Solutions can help you verify and authenticate your customers' identities, allowing users to easily and seamlessly log-in–without the need to remember any difficult phrases, complicated passwords or security question prompts. Arculus provides fully customizable security solutions that enable your customers to verify their identities or transactions with a single tap, while fortifying the security of your business in the process.

Challenges in Password Security & The Cost of Poor Password Hygiene

A maze of passwords, password managers and two-factor authentication

The first computer passwords were created in the 1960s, and most computers and systems have leveraged passwords to secure accounts ever since. Many require arbitrary characters–a mix of letters, numbers, and symbols–that provide little long-term security as many users cannot recall these complex, unwieldy passwords and often opt for easily-guessable passwords instead. And as online accounts proliferate, the sheer number of passwords that users need to remember can lead to password recycling, where users deploy the same account credentials on multiple sites. This is one of the most significant risks to password security.

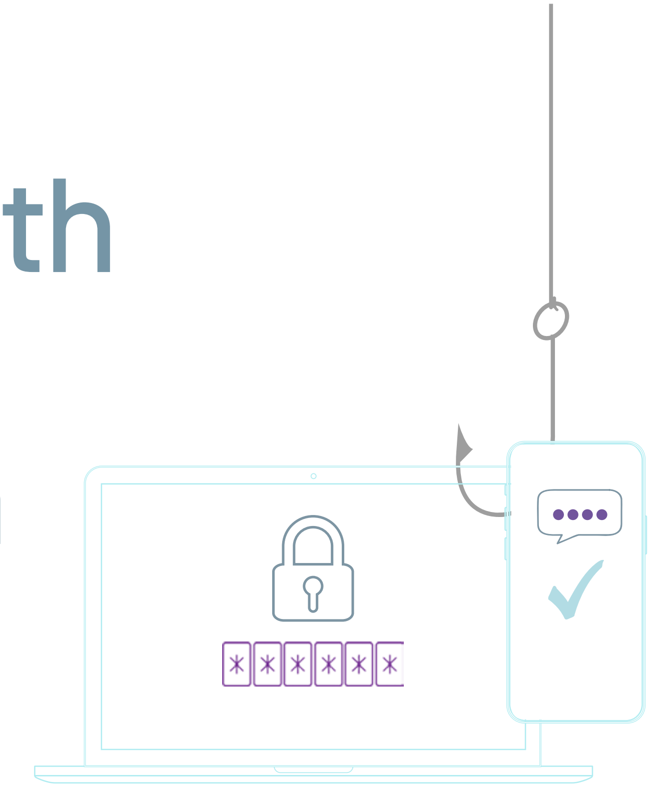
The stakes couldn't be higher for companies. Cybercrime is expected to have a $10.5 trillion[1] annual impact on the global economy by 2025, and yet, poor password hygiene remains rampant, with more than half of Americans admitting they have not changed their password in at least a year.

More than 60% of Americans surveyed say they resuse the same password across multiple accounts and devices.

Meanwhile, up to half of all company helpdesk requests involve resetting passwords, and a single password request can cost a business $70[2]. Add to that time spent on password resets–up to 11 hours per year per employee–and for an enterprise with thousands of employees, that can add up to millions in lost revenue.

1 https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/
2 https://securityboulevard.com/2022/10/the-cost-of-password-lockouts/

Challenges with Two-Factor Authentication



In recent years, businesses and customers have sought to ameliorate the password problem by using password managers. However, storing all passwords in one central location is inherently insecure as many have software vulnerabilities and bugs that can be exploited by hackers. One of the most common ways businesses try to avoid password vulnerability is the deployment of two-factor authentication–requiring users to provide an additional security measure beyond a username and password. One-time password, or links sent to a customer email or by text are a commonly used form of two-factor authentication (2FA).

But many of these systems are vulnerable. Hackers have grown smarter and now use sophisticated malware and take advantage of customer frustrations in clever and persistent ways. Hackers can hijack two-factor authentication tools and overwhelm customers with verification requests or by intercepting or spoofing one-time passwords. They then bombard a user's phone with verification requests, and to remove the flood of prompts, it's not uncommon for a busy user to hit "yes" when they are repeatedly prompted to verify their identity. And once the user hits "yes," the hackers are in.

Ultimately, passwords and security codes alone are insufficient to secure accounts, and companies need to adopt a combination of additional measures–such as biometric authentication, verification via hardware devices, or continuous monitoring–to protect themselves and their customers from malicious attacks.

Multi-factor authentication systems are harder for hackers to thwart, and when physical devices like the EAL6+ certified chip in an Arculus-powered metal card are required to authenticate, hacking becomes virtually impossible.

FIDO2: The Gold Standard of Security

Arculus Business Solutions leverages FIDO2 technology, which enables phishing-resistant authentication. FIDO is a protocol that leverages standard public key cryptography techniques to authenticate users. When a user registers with an online service, like with your financial institution, their client device creates a new key pair, retaining the private key and registering the public key with an online service. The user's system, in the case of Arculus Business Solutions, an Arculus-enabled metal card with an EAL6+ compliant chip, retains the private keys, and the public key is held on a FIDO server. Users then "sign" transactions or login with a tap of their cards to their mobile devices after unlocking the device with another authentication method, like biometrics or a PIN.

FIDO protocols protect user privacy and provide a best-in-class security experience for your users.

"I urge every CEO to ensure that FIDO authentication is on their organization's MFA implementation roadmap. FIDO is the gold standard. Go for the gold."–Jen Easterly, Director, Cybersecurity and Infrastructure Security Agency

FIDO2 can help businesses avoid the most common problems with passwords, reducing overall costs. It is a significant improvement from the past when cybercriminals could easily obtain login credentials, resulting in significant reputational, financial and operational losses for companies.

The Best Investment Is to Take a Proactive Approach to Cybersecurity

Businesses cannot afford to overlook the importance of investing in secure authentication methods, as the cost of cyberattacks continues to rise. In fact, last year alone, cyberattacks resulted in a loss of $6 trillion.[1] Failing to invest in better security measures can be even more expensive for your business, as phishing scams and cybersecurity breaches can quickly drain valuable resources.

Additionally, every time a business is hacked, customer trust is eroded and the risk of financial or identity theft increases dramatically. That harm also incurs a severe reputational cost. Customers do not want to do business with a company that cannot keep their information safe or provide protection for their data. To regain access to important IT systems, around 6 percent of businesses say they had to pay a ransom fee to hackers. Don’t let that happen to your organization.

[1] https://thecyberexpress.com/us-cyber-attacks-2023-trends/

The Benefits of Going Passwordless

1. Your customers can avoid long, complicated, and confusing passwords that they're likely to forget and that leave your systems vulnerable to hackers.

2. FIDO2 can streamline customer transactions and help authenticate customer identities and verify transactions with best-in-class security.

3. Passwordless authentication with FIDO2 provides a simple, secure login and authentication experience for your customers.

4. Increased user privacy. Your customers won't need to create security questions revealing secrets or other sensitive identifying information to your call center.

Want to Go Passwordless Today?

Reach out to us at b2b@arculus.co to schedule a demo and to learn more about how Arculus Business Solutions can work for your business.

Arculus is a trusted leader in passwordless security, developed by CompoSecure – the world's leading producer of premium metal payment cards. Our fully customized security solutions are user-friendly and simple.

Benefits of the Arculus Business Solution

Improved Security

By eliminating the need for complicated passwords and enabling one-tap signatures, the Arculus Business Solution reduces the risk of unauthorized access and ensures the security of transactions.

Enhanced User Experience

The Arculus Business Solution is easy-to-use and convenient, providing customers and employees with a streamlined log-in and transaction experience. This can improve user satisfaction and loyalty.

Customizeable Solution

Businesses can customize the Arculus Business Solutions to meet their unique needs, allowing for greater flexibility and adaptability.

Reputation & Trust-Building

By enhancing security and improving the customer experience, businesses can build customer trust and strengthen their brand reputation.

Tap-to-Transact Protection

The ability to sign transactions easily through a simple tap to a smartphone provides a fast and convenient way to authenticate transactions.

Secure Cryptographic Signing

Arculus Business Solutions offers the most up-to-date cryptographic signing via FIDO2, ensuring the highest level of security.

Cost Savings

Arculus Business Solutions can reduce the number of password recovery support requests, leading to cost savings for businesses.