DO PASSWORDS POSE A SECURITY RISK FOR YOUR BUSINESS?

Advancing technologies have been a great asset for business productivity and growth. However, they have also exposed a new set of security-related challenges. As cyberthreats continue to evolve rapidly, your business security programs and procedures must constantly improve if you want to stand a chance of protecting your critical systems and data. One of these vital security components is moving beyond single-layer security systems.

THE DANGERS OF SINGLE-LAYER SECURITY AND PASSWORDS

The "password" has been the status quo for user authentication for years. However, as our technology and communications capabilities have advanced over the years, the password on its own has failed to keep up as an adequate security measure.

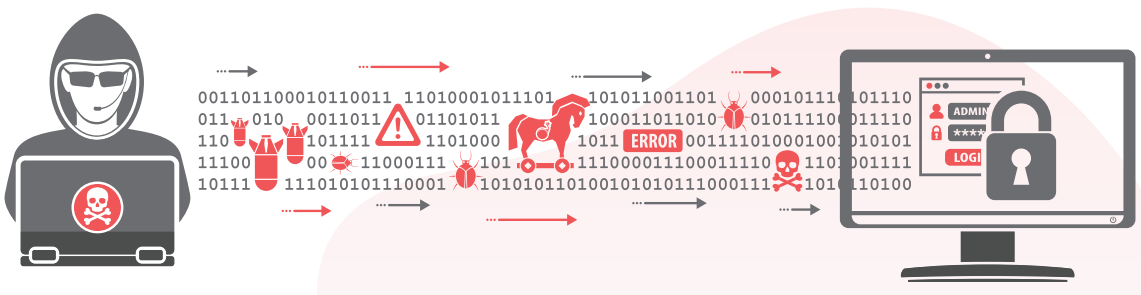
- Credentials are the most common way for a bad actor to gain access to an organization, accounting for over 60% of breaches.[1]
- In 2021, nearly a third of employees wrote down their passwords to remember them.[2]
- In 2021, only close to 5% of employees said they used a password manager.[2]
- In 2021, more than 50% of individuals reported they did not change their email passwords even once.[2]

Sources:

[1] Verizon 2021 DBIR | [2] Statista

CYBERCRIMINALS DON'T NEED A BACKDOOR WHEN THEY CAN ENTER THROUGH THE FRONT

Unfortunately, even with strict company policies requiring unique or complex passwords, relying on passwords alone for identity and access authentication can spell trouble. Password stuffing and phishing schemes easily trick users into unintentionally sharing their privileged credentials. Third-party application breaches can result in password exposure while additional cyberthreats, such as keystroke logging or brute force attacks, can be used to systematically identify or capture even the most complex passwords.



01 Experts predict that 60% of data incidents will be caused by third-party issues in 2022.[1]

02 In 2021, nearly 5% of employees who received a malicious email clicked on the link provided, exposing their organization to attackers.[2]

03 Many employees who admitted to being duped into clicking on a phishing email said it was because it appeared 100% legitimate.[2]

04 Poor password practices led to data leaks and security breaches in 30% of businesses.[3]

Sources:

[1] Forrester 2022 Predictions | [2] Statista | [3] PR Newswire

IT STARTS WITH THE USER

Users and their credentials continue to be the weakest link in cybersecurity efforts.

- Human error is involved in more than 80% of data breaches.[1]
- Insider threats affect more than 30% of businesses around the world each year.[2]

- The average global cost of insider threats has increased by over 30%.[2]
- Nearly 70% of IT leaders believe employees can expect a surge of "back to work"-related phishing emails as organizations around the world reopen after nearly two years of working from home.[3]

Sources:

[1] Verizon 2021 DBIR | [2] Swiss Cyber Institute | [3] Statista

STRENGTHEN SECURITY WITHOUT SACRIFICING CONVENIENCE OR PRODUCTIVITY

The challenge for most businesses is how to boost security without generating additional friction for its workforce or disrupting productivity. To protect the growth and success of your business, your company must create a security driven culture, starting with your employees.

Multifactor Authentication

Implement layered security strategies like multifactor authentication. Requiring users to validate their identity with more than one single-security factor, such as a username and password, allows you to maintain control over who is accessing your network and data. The use of multiple unique verification factors will exponentially reduce risks and vulnerabilities from exposed or stolen credentials.

Single Sign-On (SSO)

An SSO system enables your users to access multiple accounts and applications via a single secure login and authentication process. Once identity and access permissions are validated, the user can securely access any account managed by the SSO program from any device, at any location.

Password Server

A password server stores passwords in a centralized, secure and encrypted repository or vault, and auto-fills the password with a cached credential any time a user is challenged to authenticate it. This system allows you to enforce strong password policies and access permissions without inconveniencing your users, and boosts productivity by virtually eliminating time wasted in resetting lost or forgotten passwords.

Security Awareness Training

Conducting security awareness training for ALL users will help improve employee alertness and recognition of common cyberthreats such as phishing attempts, virulent webpages, malicious advertisements and more. After all, knowledge is power. Users that are well-trained gain a deeper appreciation of the value of security systems and will be more skeptical and cautious in their daily activities.

Let us show you how to increase security and productivity in your business.

Contact us for a no-obligation consultation.

OPTISTAR
TECHNOLOGY CONSULTANTS
A VERTEX COMPANY