PASSWORDS ARE OK!

The use of passwords is far from over. It remains to serve its purpose specially for the corporate setup despite the growing number of alternatives. As long as it is used the right way, passwords are OK!

PRIMARY USES OF CORPORATE PASSWORDS

- Windows/ Active Directory
- SAP
- Oracle
- IBM
- LDAP
- SQL

BENEFITS

- Instantly available
- Unlimited and free
- Widely used in most systems
- Recognizable to users
- Easy to change or reset if forgotten

AUTHENTICATION CATEGORIES

a. Something only I know

b. Something only I have

c. Something only I am

DRAWBACKS

- Users forget passwords
- Resetting incur costs

Security risks:

- Phishing attacks
- SPRAY attacks
- Social engineering against service desks to gain users' passwords
- Users give away or share passwords

COUNTERMEASURES

- Security awareness training
- Strong password policies
- Anti-phishing tools
- Self-service of passwords
- Password reset IT-workflow in service desks

POLICIES IN CREATING STRONG PASSWORDS

- Minimum number of characters: •••••
- Prevent use of personal identity and sequences
- Prevent use of popular passwords: password
- Many different character types: Au039:P
- Change every 3-6 months

SECURE YOUR DATA THROUGH MULTI-FACTOR AUTHENTICATION (MFA)

Combine at least two categories of supplementary authentication methods:

- SMART cards
- DUO
- Code cards
- Fingerprint
- Voice
- IRIS
- TOTP (RSAtokens)
- Face recognition
- YUBI keys
- USB tokens
- SMS
- Challenge questions
- Time-based One-Time Passwords (TOTP)

CHALLENGES FOR ALL CREDENTIALS:

- What's the cost per unit?
- Technical prerequisites?
- For BIO-credentials: Who owns and protects the bit-map? Consequences if they are stolen?
- Can the credential open all corporate applications? Can all user devices accept all credentials?
- How do you handle exceptions like a forgotten or lost credential?
- Administrative handling costs?

PASSWORDS ARE OK WHEN:

- Combined with other credentials for MFA for high-security applications
- Protection against social engineering and brute force attacks
- Used for self-service to keep costs down

"Passwords are OK when enterprises protect them and the password processes"

Finn Jensen
Chief Executive Officer, FastPassCorp

To read the full article, go to

bit.ly/passwordsareok

FASTPASSCORP