The Costs and Risks of Password Mismanagement

Some of the top Cybersecurity threats for SMBs are phishing, malware, credential theft, and ransomware. Your **FIRST line of defense is authentication**.

82% of **ransomware** attacks in 2021 targeted companies with fewer than 1,000 employees.[1]

57% of cyberattacks were **phishing**-related, to trick users into revealing sensitive information or credentials.[2]

30% of cyberattacks involve **credential theft**, due to employees use of weak or reused passwords.[3]

18% of all cyberattacks targeting small businesses are **malware** attacks.[4]

PROXIMIA®

Proximia Protections

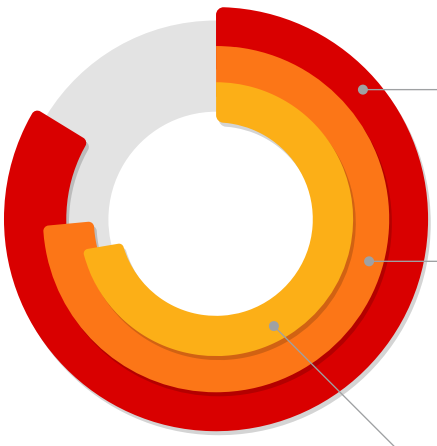
Passwordless
Users never know their passwords, so they can't reveal them.

Biometric Triggers
User identity is verified with something unforgeable.

Mutual Trust
Both user and device must approve access to the other.

Dynamic-Proximity
Users must be physically near the device they are trying to access.

Persistent Authentication
Identity is reevaluated throughout a session for ongoing protection.



80% of breaches involve **weak or stolen passwords**.[5]

74% of breaches are attributed to **human elements**, including errors, privilege misuse, and use of stolen credentials.[6]

72% of people admit to **reusing passwords**, increasing the risk of credential stuffing attacks, where hackers use stolen usernames and passwords to access multiple accounts.[7]

proximia.com | sales@proximia.com | (844) GET-PROX or (844) 438-7769

Attribution: 3, 4, 6 Packetlabs; 2 StrongDM; 1 Verizon; 5, 7 Comparitech