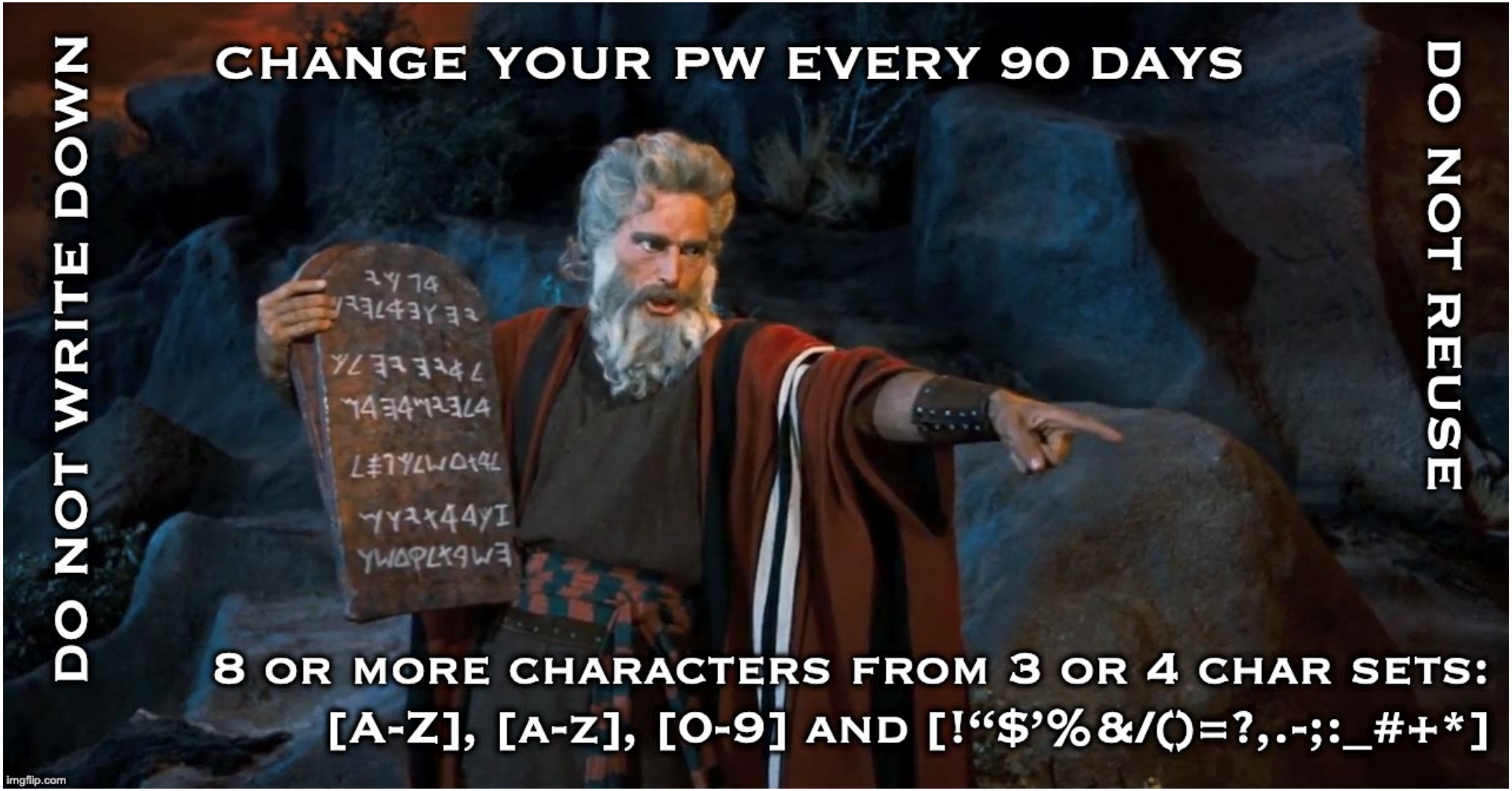
aR5z§9Qx

Modernize Static Password Policies

Vienna, 19.02.2020
KPMG Security Services GmbH

Your password must contain at least one uppercase letter, one digit, and one of the following symbols: !“$”%&/()=?,.-;:_#+*



Threat	*Traditional Mitigation*	*Not Yet Standard*
PW Guessing	strong PW, rate limit	
PW Leaking	protocol security	
Default Password	policies & procedures	
PW Hints/KBA	do not allow	
Weak PW Reset	policies & procedures	
PW Cracking	hashing	100k * PBKDF
PW Compromise	PW change	HIBP, NIST-rules
Password Reuse	not effective	MFA
Shoulder Surfing	complex PW	MFA
Phishing		X.509, FIDO

New shopping list items


Discussion

How Good Can PW-Change be Enforced?

Assumption:

- Users have many accounts

- Rules:
  - Do not reuse old PW
  - AND
  - Do not store PW with reversible encryption

Compare Hashes

-> cannot check for similarity

-> 1.am.the.Gulu || Login.4.free || 2.am.the.Gulu || Login.5.free || ..

-> + reuse at other sites

Password ToDo List for Enterprise IT

- Adopt policy for strong passwords (NIST 800-63B)
- Fraud detection
- Relax PW-change policy, e.g. 3 -> 24 months
- Make life easy for mobile users:
  Short complex PW (8+ char) OR
  passphrase (16+ char)
- Review policy + technology options for mobile PW
- Reduce reliance on passwords:
  - Strong MFA for privileged accounts
  - OTP for everybody else

NIST SP 800-63b (5.1.1.2 memorized Secret Verifiers)

- Should check passwords against previous breaches, dictionary words, simple patterns
- Should not impose composition rules
- Should provide clipboard paste functionality
- Provide an option to display the secret
- Do not enforce regular password change
- Use strong hashing (iterate PBKDF2, 32bit random salts stored in HSM)

KPMG

Rainer Hörbe

Senior Manager
Cyber Security

KPMG Advisory GmbH
Porzellangasse 51
1090 Wien

M +43 664 8595911
E rhoerbe@kpmg.at
W kpmg.at/cyber