PASSWORD MANAGEMENT

By: Johnathan Hampton

IS THEIR IMPORTANCE IN A PASSWORD?

Password Management is a key aspect to not only protection of yourself but protection of your organization.

What is a password?

- Creating and managing passwords to be as secure as possible
  - Credentials for password include:
    - Alphabetic Characters, Numbers, and Symbols

Strong Passwords

- Characteristics

Personalization

Highly recommended 12 characters or more

Shouldn't contain words in the dictionary

Weak Passwords

Common Mistakes

"password"

short passwords

Why you need a secure password?

Guessing:

Method of gaining access to an account by attempting to authenticate the user

Brute Force – using every possible combination of characters for access

Dictionary Attack -

Social Engineering

Deceiving users into revealing their username and password

How they do it?

Pretending to be an IT employee or gain trust through personalization

Never share passwords to anyone this is personal information and should be treated as so

HOW MANY PASSWORDS DO YOU HAVE?

Tiered Password System

Different Levels of Passwords

Low Security	- This is the easiest secured password for newsletter, and opportunities	Medium Security
- The second layer closest to the most secure level of password. Examples include open sites and email services.	High Security	- The last layer is the highest level of security used for financing and personal assets

- KITY: **Minimum of 8 characters**
  Must contain at least 1 upper case letter
  Must contain 1 lower case letter
  Must contain one number
  OR – 1 "special character"
  May not include the login name
  May not include personal information
- HISTORY: **Passwords may not be reused for 5 years**
- MAXIMUM AGE: **Passwords must be reset every 120 days.**
- PROTECTION: ***Sharing Is Not Permissible***
  - *Users may NEVER share a password with ANY other person, including supervisors and ITS Personnel.*
  - *Users may NEVER write their password down on a piece of paper or "post-it" note in an effort to keep from forgetting it.*

Benefits

- Flexibility - configurable to the user, group or domain hierarchy
- Increased Usability - maintains user productivity and satisfaction with a password strength meter, email calendar reminders and self-service password reset
- Increased Security - prevents both common password and code injection attacks
- Balances Usability and Security - supports both compliance and user
- Implements password best practices
- Compliance – web-based and SQL applications now meet required standards
- Cost effective – reduce password related Help Desk calls

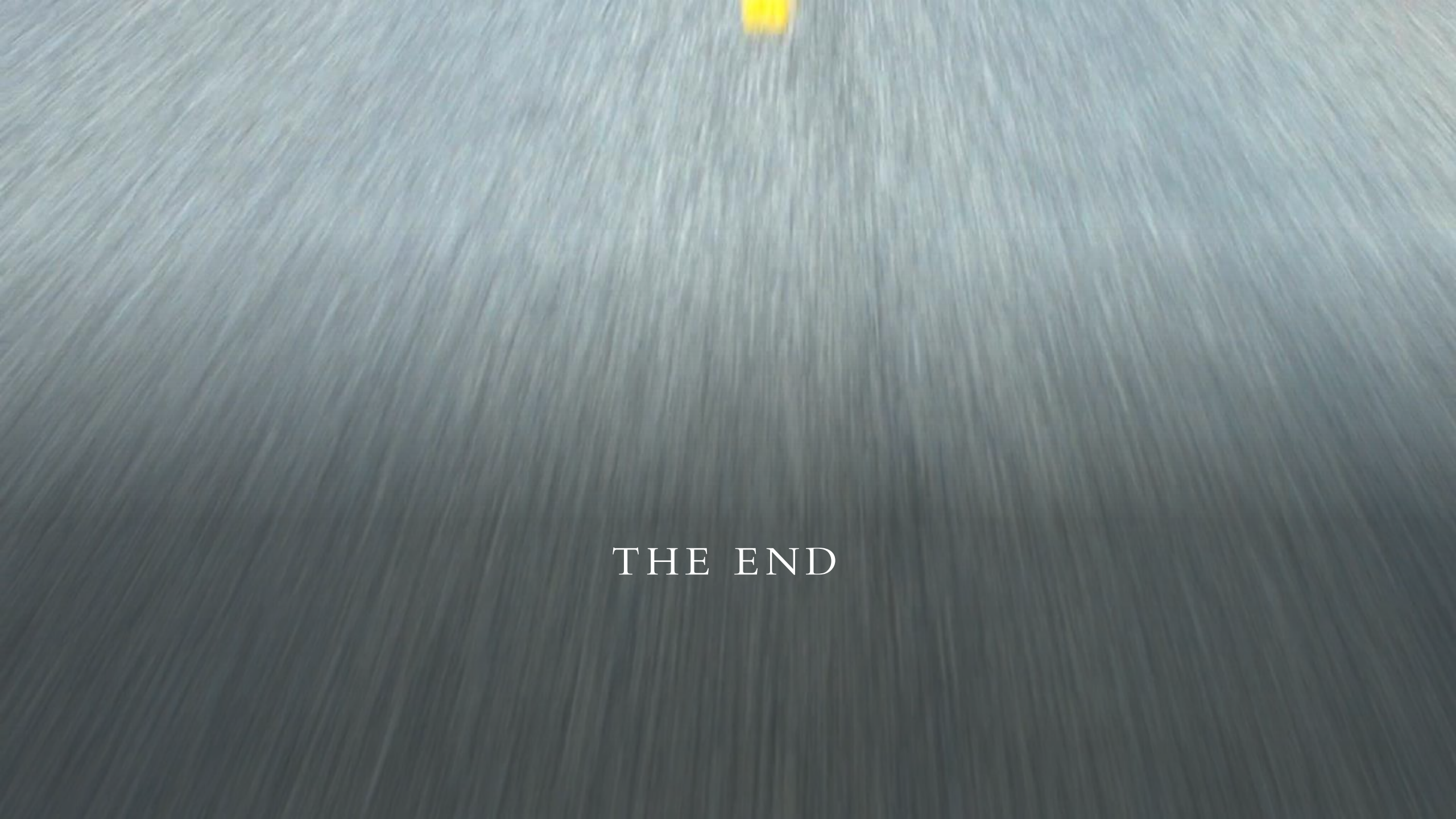

Password***

PASSWORD MANAGEMENT TECHNIQUES (WAYS TO STORE YOU PASSWORDS)

- Human memory is the safest database for storing all your passwords
- Writing passwords down on a piece of paper
- Storing passwords on a computer in a Word document or Excel file
- Password Manager is software that allows you to securely store all of your passwords and keep them safe, typically using one master password. This kind of software saves an encrypted password database, which securely stores your passwords either on your machine or on the Web.
  - *You should not rely totally on any type of password manager*

ADDITIONAL TIPS TO SECURE YOUR IDENTITY

- Open Wi-fi connection can be easily hacked using a free packet sniffer software
- Always enable “HTTPS” (also called secure HTTP) settings in all online services that support it – this includes Twitter, Google, Facebook and more.
- Spoofed Website


THE END