Donna Batchelor
Passwords blog post sample
[Month] 2023

OuamdEAP1849!: Turning Randomness Into Real Security

Did my dog jump on the laptop, or is it time to remind our [industry] users of the need for a solid password management strategy?

Today, 82% of successful security breaches involve the human element. In a recent cybersecurity report, 80% of respondents said their organization suffered one or more breaches that they could attribute to a lack of cybersecurity skills or awareness.
The same report showed that 64% of organizations lost revenue due to breaches in the past year; 38% reported that breaches cost them more than a million dollars.

Our online portal is where you manage your company's [critical assets]. Access to it should be granted judiciously. Great care should be taken to secure that access with strong, frequently changed, and safely guarded passwords.

Simple phrases or words from your life may not be the best options — your colleagues and employees probably know your pets' or kids' names, your favorite baseball team, or your phone number. They may even know your birth date, the street you live on, or your alma mater. Passwords like Fido123, Susie5551234, or GoDiamondb@cks! aren't the best choices to protect your company's [critical assets].

The password above? Not the dog … more like my raven.

> *"Once upon a midnight dreary, while I pondered, weak and weary,*
> *Over many a quaint and curious volume of forgotten lore—"*

Recognize that? It's the beginning of "The Raven" by Edgar Allan Poe. The crazy jumble of characters in the title of this post is a password I've used in the past (and can now never use again!). "Ouamd" are the first letters of the first five words of the poem. Poe's initials are "EAP." He died in 1849. If possible, always include a special character—in this case a bang, or exclamation point.

To be as secure as possible, passwords should be something easy for you to remember and hard for others to guess. Other tips to keep in mind:

- Use your [industry] online portal password only on that site … and nowhere else.
- Avoid using words, English or otherwise, that can be found in a dictionary.

- Keep your password to yourself, please! Don't place it on your computer monitor, office wall, or on a piece of paper hidden under your keyboard or mouse pad.
- Create a new password every time.
- Be aware of your surroundings when using your mobile device in public to access your [industry] services.
- Change your password often. Your company can choose to have your portal passwords expire every 30, 60, 90, or 120 days—the default is 60 days. Remember that this setting applies to all users in your company. Your sales officer can help change it to a different interval.

[Client name] takes myriad measures to protect your [critical assets]; however, it takes a password to get in. Consider your own password, and reiterate to other users the need to create strong [industry] online passwords and safeguard them. Make your password so difficult that it screams to any would-be hacker: "Nevermore!"

Disclaimer: Do not use "OuamdEAP1849!" as your password!