Type “Password Meme” in Google, and the results will range from the comical to the profane.

The consensus? People hate everything about passwords—changing them, trying to come up with good ones, remembering them. . . . Well, you get the idea.

At the same time, passwords are the first and last line of defense in the battle to protect our mobile devices, networks, accounts and personal information.

However, yesterday’s algorithms that require so much complexity that it is impossible to remember all your passwords (and, as a result, you reuse them everywhere) are not necessarily the best way to go.

In this issue we will cover new approaches and resources for password creation and protection. Read on for tips on avoiding headaches as you protect your data.
Reassessing Password Strength

By Gary Windham, Senior Enterprise Systems Architect
Integration Infrastructure and Architecture

Over the past few years, I have received voluminous feedback from UA’s 24/7 IT Support Center regarding the NetID password strength policy and implementation. Close to 30% of the 24/7’s support calls are password-related. Regardless of your role at the University, you’ve probably had numerous aggravating experiences selecting a “strong” password.

The “conventional wisdom” for password strength architecture has, until recently, forced users to create passwords that may be difficult to guess, but are easy to forget. You were directed to include four character “types” (upper and lower case letters, numbers, and special characters) in combinations that were nonsensical, but were tough for hackers to crack.

There is no question that strong passwords are a must. But there is a shift in thinking as to what constitutes strength.

The rise of social media, MMORPGs (Massively multiplayer online role-playing games), and consumer-oriented cloud service sites -- most of which manage their own databases -- have resulted in several large scale data breaches, in which millions of account credentials have been disclosed (and the arsenals of attackers significantly augmented). UA’s new two-factor authentication system, NetID+, is a direct response to this “new normal”. However, like many security-related issues, the required response is multi-faceted; strong passwords are still relevant, and continue to play an important role in securing access to data and services.

The following XKCD comic (broken into two parts) brilliantly illustrates what has been the conventional wisdom for passwords:
Reassessing Password Strength, Continued

So, what should we be doing differently? We need to provide a holistic approach to password strength, which continues to provide strong technological enforcement of password strength policy, while making password creation and memorization easier.

Here is the second part of the comic, which provides a sample of an easier password to type and remember, but that is much harder to guess than the one above:

![Password Strength Comic](image)

Passwords aren’t going away any time soon. But we can make the whole process much less painful.

Pro Tips:

1. The website [http://correcthorsebatterystaple.net/](http://correcthorsebatterystaple.net/) is very handy for generating this type of password “on the fly”, and allows you to fine tune the length, separator characters, etc.

2. The “Generate password” button on the NetID Password Change and Reset pages (featured later in the newsletter) will generate a password using a variant of the “correct-horse-battery-staple” algorithm. Feel free to click it repeatedly until it provides you with a suggestion that “clicks” with you!

---

No More Random – Passwords Are Better With a Twist!

New suggestions for selecting a password reflect the shift away from random characters that are hard to remember (and possibly easy to guess) to a longer password. Here are just a few tips that will help you create a strong password:

- **Longer is stronger.** The best passwords are at least 10 characters in length.
- **Use a phrase.** Pass phrases are easy to remember, but difficult to guess, and you can use spaces as a special character when selecting your NetID password.
- **Misspell a word or two.** Make a note of what was misspelled until typing the pass phrase becomes a habit (usually within a few days).
- **Consider using a nursery rhyme, movie quote, or song lyrics, and then put a twist on it** (e.g., “The green cow jumped over the moon!”).
NetID Website – What’s New?

Have you changed your NetID password lately? If you haven’t, you will be in for some pleasant surprises. Netid.arizona.edu is a one-stop shop for all things NetID, including the following:

- Creating your NetID
- Managing passcode settings
- NetID+ (UA’s two-factor authentication system) management
- Troubleshooting NetID problems
- News, FAQs, and policies

But you will also find that PASSWORD CHANGES ARE EASIER!

The process, complete with tips, random password generator, and “strength-o-meter,” guides you to successfully creating a 360-day NetID password.

Choose Password Page

The page where you create or change your password has had a major facelift.

1. Included on the page is a “random password generator,” which you can use to create a 360-day password. Keep “clicking” until you see one that will resonate with you and be easy to remember.
2. Tips for selecting your own password that will get you to the “360 day goal.”
3. After you have selected your password (whether randomly generated or created on your own), you can get the instant gratification of knowing that you won’t have to go through this process again for almost a year.

Choose Password

Suggestions for a strong, memorable password:
- Use a generated password:
- Make sure it is 10 or more characters long, includes capitalization, spaces, and some punctuation.
- Use a "pass phrase" instead of a password.
- Think of nursery rhymes, songs, slogans, mottos.
- Pick a phrase or a sentence that you can remember.
- Misspell a word or two for added strength.
- Some examples: This and That! ...Went up the Hill Meet me in St. Louis

What is a UA NetID?

Your UA NetID is your personal identifier many online services at the University of Arizona. Some of these services include:

- E-mail and computing accounts (UAConnect, HPC)
- UAccess applications (Student, Employee, Analytics, etc.)
- New Employee Resources and Benefits Enrollment
- University site-licensed software
More Password Tips

- Use a unique password for each of your important accounts.
- NEVER share your passwords with others.
- Don’t enable “remember password” functions on websites, ESPECIALLY on public computers.
- Too many passwords to remember? Consider using a Password Manager, where you can store passwords for all your accounts. There is one caveat to this: make sure you create a very strong password to protect your information, and then REMEMBER IT!
- Whenever and wherever you can, use two-factor authentication.

For more tips, visit our Password Security page!

Be Cyber Aware!

STAY INFORMED ON

INFORMATION SECURITY

ISSUES
TRENDS
ALERTS

Sign up for UA Information Security’s listserv.
Open to all faculty and staff.

DID YOU KNOW?

UA faculty and staff are required to complete all-employee security awareness training. Request access to our training on our SANS Securing the Human webpage.

Would you like to promote security awareness in your department? Download our custom screensavers!

THINK BEFORE YOU CLICK

In one year the number of malicious web links grew by nearly 600%

Like us on Facebook
Follow us on Twitter