Cybersecurity Awarenes Month

Cybersecurity Awareness Month

Office of Information Technology / Division of Information Security

Shining Light on Password Safety

Welcome to Cybersecurity Awareness Month (CSAM)! CSAM is an international campaign from the Cybersecurity and Infrastructure Security Agency (CISA), and the National Cybersecurity Alliance (NCA), that happens every October. Now in its 21st year, the CSAM effort helps spread awareness about cybersecurity best practices and challenges everyone to think critically about cyber safety.

Each week in October, the Indian Health Service (IHS) Division of Information Security (DIS) will highlight a different subject related to cyber safety through various outreach tools. The first week of CSAM is all about passwords and password safety. Read the document to the end for a fun craft activity!

Long, Strong, Random, Unique Passwords

Most activities performed in modern technology require users to prove they are who they say they are, and almost all security efforts have one thing in common – passwords. Strong passwords are your first line of defense against cybercriminals and data breaches.

With passwords being such an essential part of cyber safety, let us shine some light on how to create a strong password. Strong passwords have three things in common: long, random, and unique.

Long Passwords

The longer a password is, the harder it is to guess and therefore the safer that account or device becomes. Passwords should be at least 16 characters long and contain uppercase and lowercase letters, numbers, and symbols.

Random Passwords and Passcodes

In addition to being long, passwords should be random. They should not consist of just words in the dictionary or contain personal information that is easy to guess, such as your name or birth date. For example, the password *cXmnZK65rf*&DaaD* is much harder to guess than *IHSpassword1234!*

To help remember your password while keeping it secure, you can also create a passcode. A passcode is a series of unrelated words strung together with numbers and symbols. An example of a strong passcode is *HorsePurpleHatRunBay39465?!^@*.

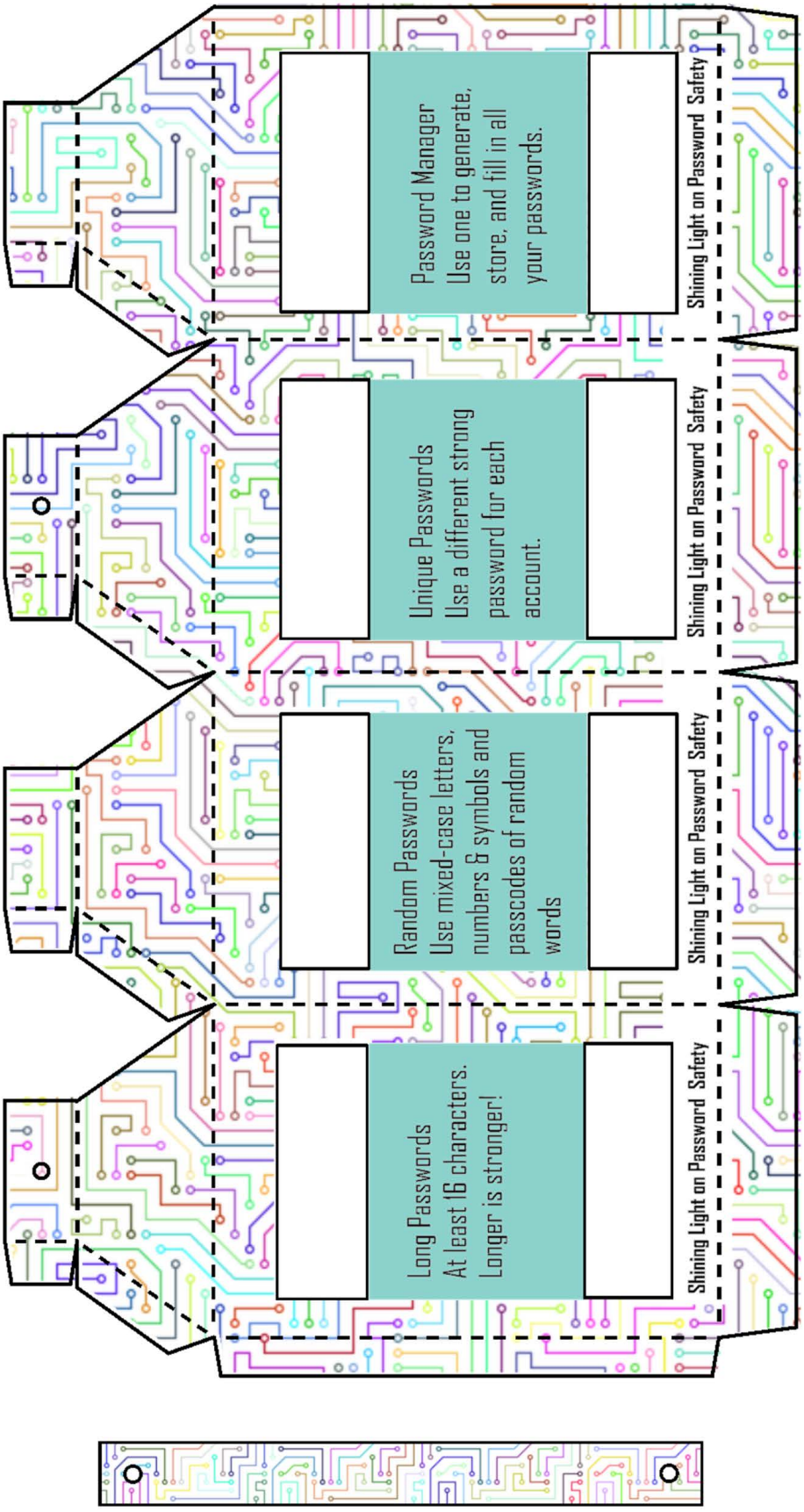
Unique Passwords

It is essential to use a different password for each account you create or device you secure. This keeps bad actors from compromising multiple accounts at the same time. According to a 2023 report from CISA, only 38% of people use unique passwords for all their accounts. Using the same password for multiple accounts is not safe, even if the password is strong.

Password Managers

While *cXmnZK65rf*&DaaD* is a great password to secure your account with, it is hard to remember. Keeping track of all the passwords and passcodes for all your accounts and devices may feel impossible. You may be tempted to write them down, or save them in a document on your device. This is a bad idea because if your device is compromised, so are all your passwords.

In comes a password manager, which is an easy-to-use program that generates, stores, and fills in all your passwords. Password managers tell you when you have weak or re-used passwords and can generate strong passwords. They can also automatically fill logins into sites and apps. The password manager is secured by its master password, so only you can access it. When you use a password manager, you are much more likely to use a long, random, and unique password on every site and that makes it much harder for someone to steal your valuable information. Using a password manager will require you to remember only one password, which will give you access to all of your other passwords.



Shining Light on Password Safety: Activity

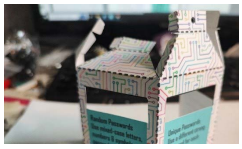
Print out and assemble this paper password lantern! It contains a reminder of the four important password safety subjects discussed in this document. Just print, cut, fold, and add a battery-operated candle to help shine a light on the importance of strong passwords!

Materials

- One sheet of 65 lb. cardstock (copy paper will also work, but not as well)
- Scissors or a craft knife
- Glue or tape
- Battery operated candle or light
- Paper fasteners (optional)

Directions

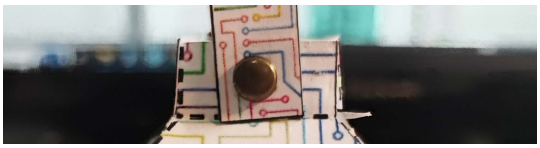
1. Print out the last page of this document. Normal copy paper will work, but for best results print on 65 lb. cardstock.
2. Cut along the solid lines.



3. Assemble the lantern by folding the paper along the dotted lines.
4. Use glue or tape to secure the body of the lantern.

5. Use glue or tape to secure the top of the lantern.

6. Secure the handle with paper fasteners. Alternatively, tape or glue the handle on.



7. Insert a battery-operated candle or other light into the lantern. Now you have a beacon of protection against cyberattacks!

Note: DO NOT use an open-flame candle with this lantern.

Have a cutting machine, like a Cricut® or Silhouette®? Download this SVG file to use with your machine's software to cut out the lantern. ***This is not required, but optional.***