World Password Day:

Observing and Strengthening Cybersecurity

Office of Information Technology
Division of Information Security
APRIL 2024

There is never a bad time to create or maintain strong passwords to enhance cybersecurity. Did you know that May 2nd is World Password Day? World Password Day was established to raise awareness of the vital role passwords play in safeguarding our digital lives.

World Password Day was created by Intel Security (now McAfee) in 2013 as a part of a campaign to raise awareness about the importance of password security and encourage people to create stronger passwords.

Strong passwords are crucial because they serve as the first line of defense against unauthorized access to our sensitive information. Whether it is personal email accounts, social media profiles, or work-related platforms, strong passwords play an important role in protecting data from cybercriminals. These bad actors are invited into your life when you use weak or simple passwords, which allows them to exploit you and access your accounts.

Regularly changing your password is important because it helps prevent unauthorized access to your account, even if it is compromised. If a cybercriminal obtains your password through a data breach, promptly changing your password can hinder their attempts to access your account. Also, changing your password regularly reinforces good security habits and enhances the overall security of your accounts.

Reusing the same password across multiple accounts creates serious security risks. If a hacker compromises one account, they could potentially access all other accounts using the same password. Using a unique password for each account reduces the chance of identity theft.

91% of people understand that reusing passwords is a security risk.

More than **80% of confirmed** breaches are related to stolen, weak, or reused passwords.

On average, it takes **14 seconds** to type out a password.

Only half of internet users are somewhat familiar with best practices of password security.

Nearly **60% of individuals** make their passwords stronger as a result of noticing unauthorized access to their accounts or devices. .

In 2022, over 24 **billion passwords** were exposed by hackers.

Internet users who don't use password managers are **three times more likely** to be affected by identity theft.

Sources:
Norton.com

Password managers are helpful tools for securely storing and managing passwords. They allow users to create strong, unique passwords for each online account and store them in an encrypted vault. With a password manager, users only need to remember one master password to access all of their stored passwords. This eliminates the need to memorize difficult passwords, reuse passwords, or write them down.

Here are some tips for creating strong passwords:

- Create complex passwords by using a combination of random uppercase and lowercase letters, numbers, and special characters to make it harder to guess.
- Consider using passphrases, which are longer combinations of words or phrases that are easier to remember but harder to guess.
- Avoid using common patterns, such as sequential numbers, common words, or personal information like birthdays or names. This prevents easy to guess passwords.
- Whenever possible, enable two-factor authentication to add an extra layer of security to your accounts. Two-factor authentication requires both a password and another way to confirm your credentials.

How to observe World Password Day:

- Use World Password Day to set a calendar reminder to update all passwords and review the security settings for your online accounts including work, social media, email, banking, and shopping accounts.
- Educate others by spreading awareness about password security. Talk to your family, friends, and coworkers. Share tips for creating strong passwords and encourage them to prioritize password security in online activities.
- Encourage people to use two-factor authentication on their accounts whenever possible to enhance security measures beyond passwords.
- Raise awareness about the benefits of using password managers to secure store and manage passwords.
- Participate in online forums, discussions, or initiatives dedicated to cybersecurity awareness and password security.
- Don't write down your passwords or PINs in plain sight, and make sure to shield your keyboard or keypad from others when you log in.
- Don't share your passwords, the answers to password reset questions, or multi-factor authentication codes sent in text messages. IHS IT staff will never ask you for your passwords or multi-factor authentication codes.

As we approach World Password Day, let's maintain our commitment to strengthening cybersecurity by adopting best practices for creating and managing secure passwords. By prioritizing password security and remaining vigilant against cyber threats, we can protect our online accounts from unauthorized access and potential harm. Remember: a strong password serves as the first line of defense against cyberattacks.

NOTE: The links and products in this document are for informational purposes only and do not signify an endorsement.

Please contact cybersecurity@ihs.gov with any questions or comments about this newsletter.