

# Drip7 Offers 10 Keys to Enhance Security on February 6, Internet Safety Day

*Internet Safety Day provides an opportunity to review personal practices to improve safety on the internet.*

SPOKANE, WA, UNITED STATES, February 6, 2024 /EINPresswire.com/ -- "Individuals need to educate themselves on safe internet use. Ask for training at work. Share the knowledge with family, particularly the young and elderly," stated [Heather Stratford](#), [Drip7](#) Founder/CEO.



Staying safe on the internet is crucial in today's digital age. Here are some best practices to protect oneself online at home and work:

“

Individuals need to educate themselves on safe internet use. Ask for training at work. Share the knowledge with family, particularly the young and elderly”

*Heather Stratford, Drip7  
Founder and CEO*

## Use Strong and Unique Passwords:

- Create complex passwords that include a mix of uppercase and lowercase letters, numbers, and symbols, the longer, the better.
- Avoid using easily guessable information like birthdays or common words.
- Use a unique password for each online account. More than 60% of Americans use the same password for more than one account.[1]

## Enable Two-Factor Authentication (2FA):

- Enable 2FA whenever possible to add an extra layer of security to an account. Multi-factor Authentication (MFA) can stop 96% of bulk phishing attacks.[2]
- This usually involves receiving a code on a phone or email in addition to entering your password. 73% of people believe smartphones are the most

convenient MFA method.[3]

#### Keep Software and Systems Updated:

- Regularly update operating systems, antivirus software, browsers, and other applications. 1 in 5 internet users have experienced a virus attack.[4]
- Updates often include security patches that protect against newly discovered vulnerabilities.

#### Be Cautious with Emails:

- Avoid opening emails from unknown senders.
- Be wary of email attachments and links, especially if the email seems suspicious.
- Verify the legitimacy of unexpected emails before clicking on anything. Phishing email statistics suggest that nearly 1.2% of all emails sent are malicious, which in numbers translates to 3.4 billion phishing emails daily. [5]

#### Use Secure Websites (HTTPS):

- Look for "https://" in the URL and a padlock icon in the address bar before entering personal information.
- Avoid entering sensitive information on websites that do not have secure connections. According to Google's Transparency Report, roughly 93.2% of browsing time on Chrome is spent on HTTPS pages that have legitimate digital certificates.[6]

#### Install and Update Security Software:

- Use reputable antivirus and anti-malware software to protect a computer from threats.
- Keep the security software up to date to ensure it can detect and block the latest threats. Seventy-five percent of security professionals said they have seen an uptick in attacks over the past year, with 85% attributing the rise to bad actors using generative AI.[7]

#### Regularly Back Up Your Data:

- Backup important files regularly to an external hard drive or a secure cloud service. With that in mind, it comes as little surprise that only 10% of IT users backup their computer data daily.[8]
- In case of ransomware or other data loss, the information can be restored from a backup. According to Verizon, ransomware attacks were involved in 24% of all breaches.[9]

#### Educate oneself on Phishing:

- Be aware of phishing attempts where attackers try to play tricks allowing sensitive information to be revealed. Phishing is the most common form of cyber-crime, with an estimated 3.4 billion spam emails sent every day.[10]
- Verify the legitimacy of websites and emails before providing any personal or financial information. Phishing accounts for 39.6% of all email threats. [11]

Use a Virtual Private Network (VPN) for Added Privacy:

- Consider using a VPN, especially when using public Wi-Fi, to encrypt internet connections and protect data from potential eavesdroppers. Of those using a VPN, 66% use a VPN to help protect personal data.[12]

Teach Internet Safety to Children:

- Have children? Educate them about internet safety, including the risks of sharing personal information online. Some alarming statistics on children and internet safety reported by Zipdo include: 27% of children 7-17 years old have encountered harmful content online. One in 25 youth received an online sexual solicitation in which the solicitor tried to make offline contact. 62% of children who experience online bullying do not report the incident to their parents.[13]

Safer Internet Day began 20 years ago in the EU (European Union). It has since spread globally. In the U.S., last week, a Senate committee questioned leaders of five of the leading social media companies specifically on internet safety for children. The Senate is considering increasing the guardrails for children. Chew, CEO of TikTok, disclosed that more than 170 million Americans use TikTok monthly.

By adopting these practices, one can enhance online security and minimize the risks associated with using the internet. Always stay vigilant and be cautious when interacting online.

- 1 <https://www.zippia.com/advice/mfa-statistics/>
- 2 <https://gitnux.org/two-factor-authentication-statistics/#:~:text=protect%20their%20data,-2FA%20can%20block%20100%25%20of%20automated%20bots%2C%2096%25%20of,99.9%25%20of%20account%20compromise%20attacks.>
- 3 <https://www.zippia.com/advice/mfa-statistics/>
- 4 <https://www.safetymdetectives.com/blog/antivirus-statistics/>
- 5 <https://sprinto.com/blog/phishing-statistics/>
- 6 <https://www.globalsign.com/en-sg/blog/certificate-authority-101-a-glossary-of-key-terms#:~:text=CAs%20are%20entrusted%20to%20make,that%20have%20legitimate%20digital%20certificates.>
- 7 <https://www.deepinstinct.com/voice-of-secops-reports>
- 8 <https://expertinsights.com/insights/cloud-backup-stats/>

- 9 <https://www.techtarget.com/searchsecurity/feature/Ransomware-trends-statistics-and-facts>
- 10 <https://aag-it.com/the-latest-phishing-statistics/>
- 11 <https://www.hornetsecurity.com/en/cyber-security-report/>
- 12 <https://www.forbes.com/advisor/business/vpn-statistics/>
- 13 <https://zipdo.co/statistics/online-safety/>

Deb McFadden

Drip7

+1 203-856-4046

PR@drip7.com

Visit us on social media:

[Facebook](#)

[Twitter](#)

[LinkedIn](#)

[Instagram](#)

---

This press release can be viewed online at: <https://www.einpresswire.com/article/686458739>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2024 Newsmatics Inc. All Right Reserved.