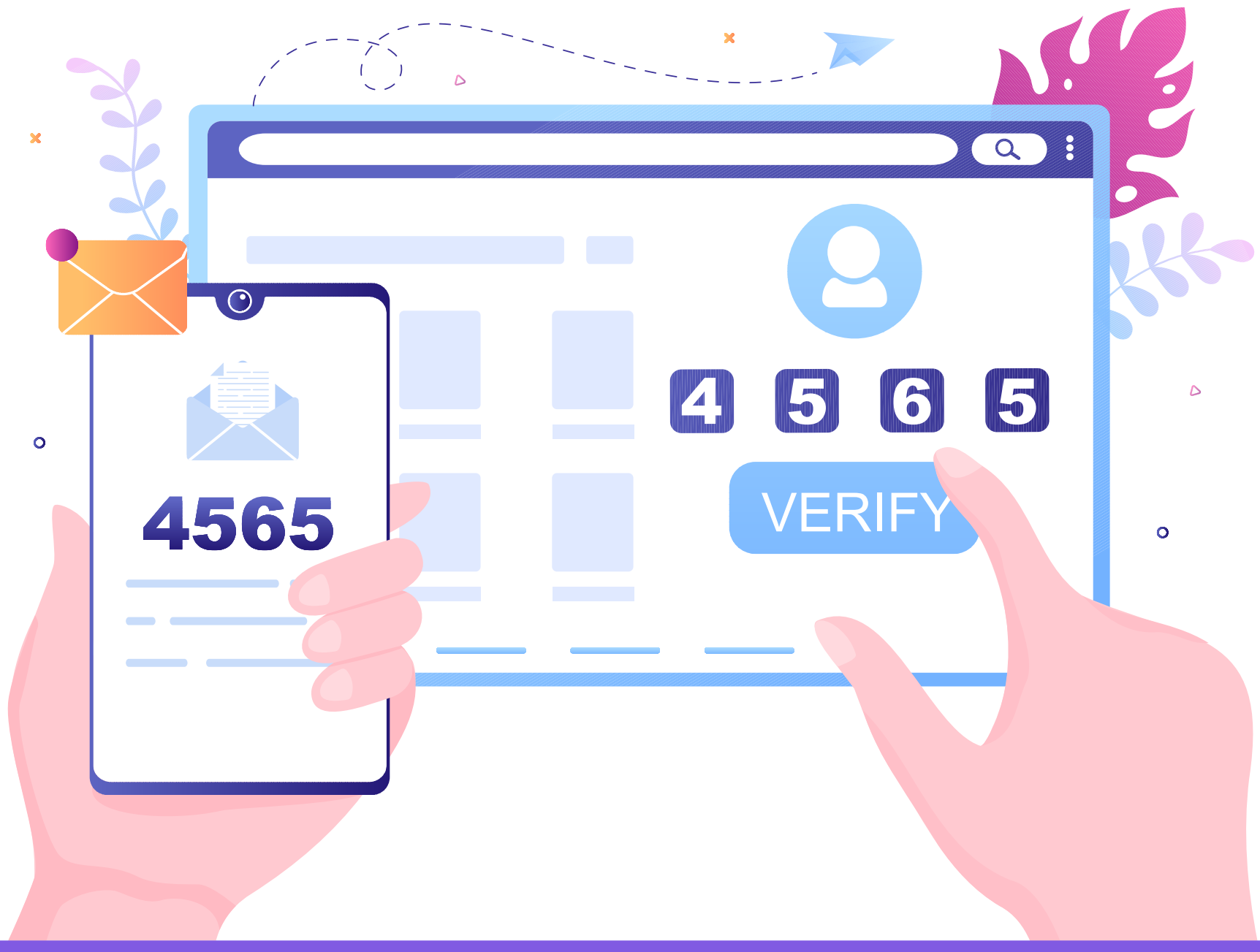
ONLINE SECURITY

SAFE JOURNALISM IN THE ONLINE WORLD

Today, it is almost impossible to imagine journalism without the use of modern communication methods conducted via the internet. On one hand, the internet has made communication easier, while on the other hand, it has presented us with new challenges. Security in the online world is one of the key challenges journalists face on a daily basis. Whether you are experienced in this field or encountering it for the first time, this guide should serve as a small reminder of what to pay attention to when it comes to online security. The information in this guide is general, and you may need to adapt certain aspects to your own way of working or conduct further research. Keep in mind that different tools, applications, and protection methods are used in different situations and types of work. There are no perfect tools, perfect applications, or perfect ways to stay safe online. This guide* provides basic guidelines for journalists to help protect their data and information when working on the internet.

* This guide was created as a result of a series of workshops and lectures within the Journalist Security Fellowship project, implemented by Internews in Croatia. Internews is an international nonprofit organization that supports independent media in over 100 countries worldwide. The guide was compiled by Monika Kutri, a participant in this program.

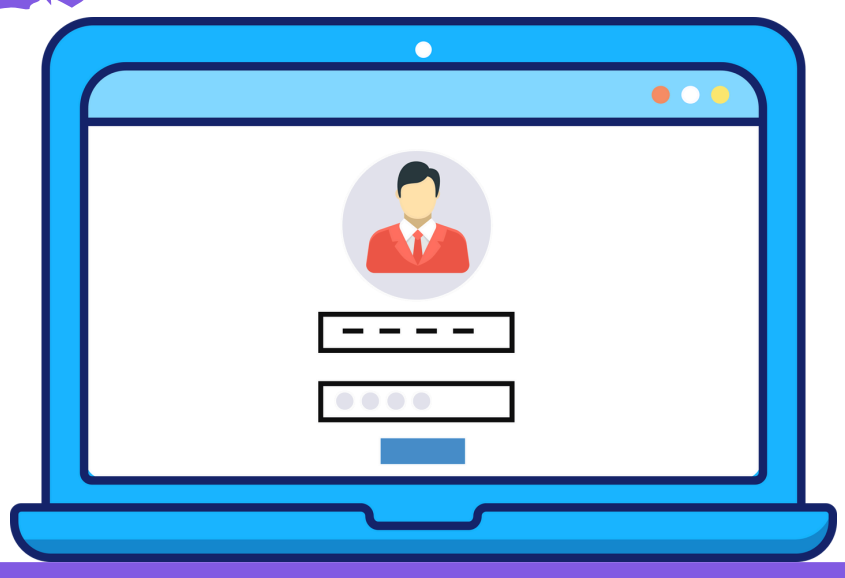
TWO-FACTOR AUTHENTICATION



Enable two-factor authentication (2FA) for an extra layer of security. 2FA is a method of verifying your identity using two separate forms of authentication. For example, when logging into your bank account, you enter your username and password (the first factor), followed by a one-time code sent via SMS (the second factor). This significantly increases login security and reduces the risk of unauthorized access.

Many services now offer 2FA as an option, and it's highly recommended to enable it on all accounts where it’s available.

STRONG PASSWORDS



Use strong, unique passwords for each of your accounts. A secure password should be long and include a mix of uppercase and lowercase letters, numbers, and special characters. When it comes to password strength, length matters most. A passphrase made up of several random words is a great option.

Make sure to use a different password for every account - if one is compromised, your other accounts will still be protected.

The easiest and safest way to manage multiple complex passwords is by using a password manager.

A password manager is an app that securely stores all your passwords, generates strong new ones, and only requires you to remember one master password to access the rest.

Suggestion:

- **1Password (free for journalists)**
- **KeePassXC**
- **Bitwarden**

ENCRYPTION

Encryption is the process of converting readable information (plaintext) into an unreadable format (ciphertext) using mathematical algorithms and encryption keys. It is used to protect data and ensure user privacy across various areas, including:

- Communication:

Encryption is widely used in communication apps—such as email, messaging, and VoIP—to safeguard the information users exchange. It prevents unauthorized access and ensures that only the intended recipient can decrypt the messages. Apps like WhatsApp and Signal use end-to-end encryption for this purpose.

- Data Storage:

Encryption protects sensitive data such as financial records, medical information, personal identification documents, and other confidential content stored on devices or in databases.

- Network Security:

Encryption plays a key role in securing data transmission over networks. For example, the HTTPS protocol uses SSL/TLS encryption to secure web traffic, while VPN services encrypt internet traffic to protect user activity and maintain privacy online.

Use encryption to protect sensitive information such as private messages, files, or emails. There are various tools and services available that can help you encrypt your data and keep it secure.

End-to-end encryption is a method of encrypting data during communication between two parties, ensuring that only those two parties can access the content of the conversation. This means that even the service provider facilitating the communication cannot read the encrypted data. Messaging apps can use end-to-end encryption to ensure that messages shared between users remain private.

Keep in mind that this system is only secure as long as the devices being used are physically secure. For example, the person you're communicating with could take a screenshot of your conversation or show it to someone else in person. Always be aware of this risk when discussing confidential matters. Also, if you're backing up your data, note that some apps require you to manually enable encryption for backups. Be sure to check your settings and ensure that backups are protected as well.

USE OF SECURITY SOFTWARE

Use antivirus programs, anti-malware tools, and other security software to help protect your computer from malicious threats. Make sure to keep all software up to date to ensure you have the latest security patches. If you're using Windows, make sure Windows Defender is enabled.

SAFE BROWSING

When working online, always connect through secure networks that are password-protected and encrypted. Avoid using free or public Wi-Fi networks that are open to everyone, as they are highly vulnerable to hacking and eavesdropping.

Use a Virtual Private Network (VPN) when connecting to the internet. A VPN encrypts your internet connection and allows you to browse safely and anonymously. This is especially important when accessing the internet via public Wi-Fi. A VPN creates a private, encrypted tunnel between your device and the internet, ensuring that all data transmitted is secure. It also masks your IP address by replacing it with the VPN server's IP, helping to protect your identity and privacy online.

VPN suggestion:

Tunnel Bear

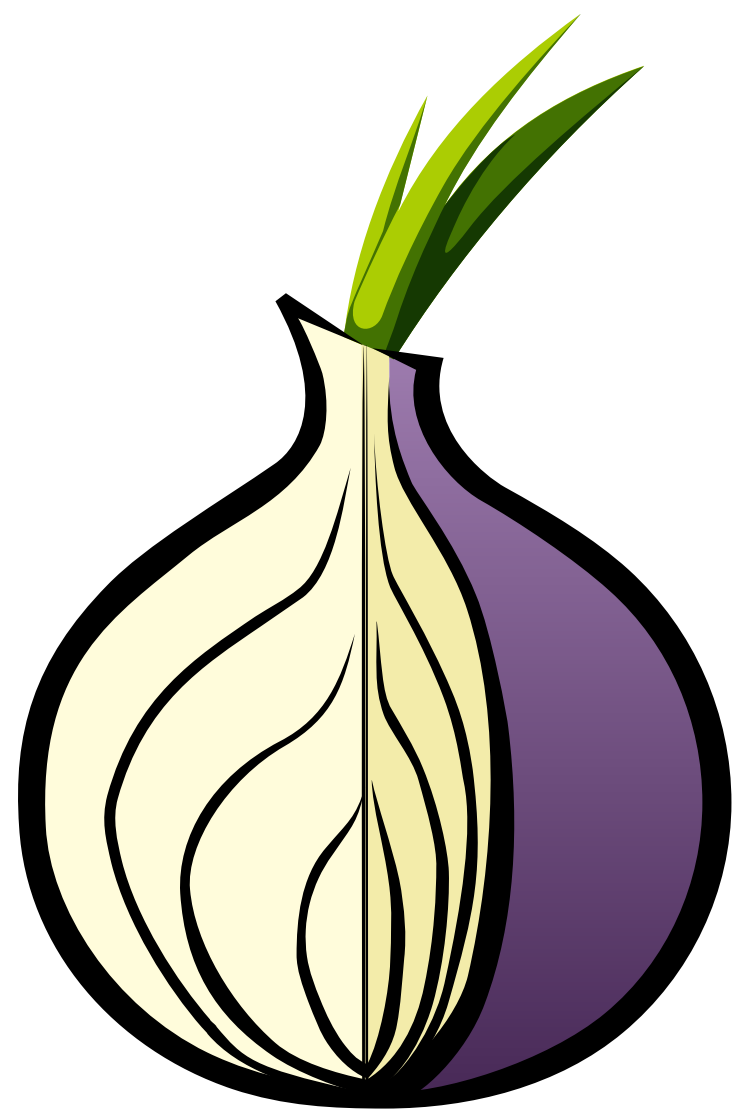
Mullvad

ProtonVPN

TOR is a free software that enables anonymous browsing on the internet by routing traffic through a decentralized network of volunteer-operated servers. It uses specialized encryption and traffic redirection technologies to hide the user's identity and provide secure access to the web.

The TOR network works by passing user traffic through a series of nodes (also called relays) before it reaches its final destination. Each node only knows the previous and next node in the chain—it does not know the origin of the traffic or its final destination. This structure allows users to visit websites, exchange messages, and transfer data anonymously and securely.

It is important to note that TOR is sometimes associated with illegal activities such as drug and weapons trafficking, the sale of stolen data, or hacking services. While TOR can certainly be used for legitimate purposes - such as protecting the identity of journalists, activists, or whistleblowers - it should always be used responsibly and in accordance with applicable laws and regulations.



Before entering sensitive information such as usernames, passwords, or credit card numbers, make sure the website's URL is secure and familiar.

HTTPS (HyperText Transfer Protocol Secure) is the secure version of HTTP, the protocol used for communication between your web browser and a website. When a site uses HTTPS, your connection is encrypted, meaning all data transferred between your browser and the web server is protected from unauthorized access.

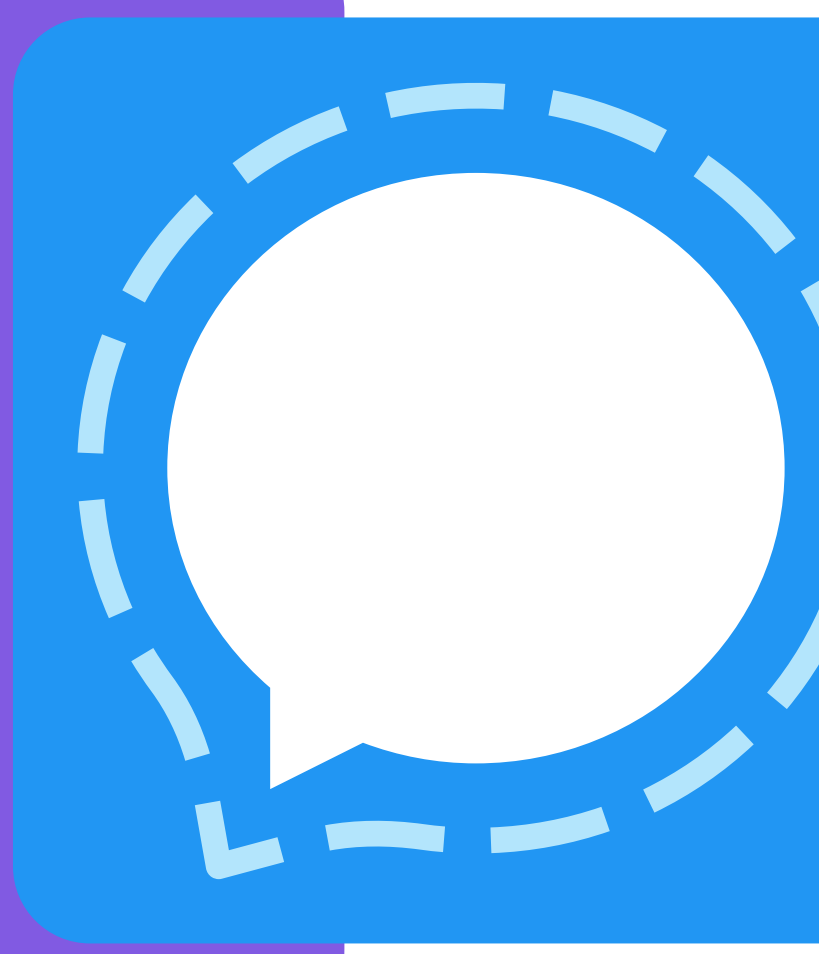
Most modern browsers display a padlock icon—usually green or closed—next to the URL in the address bar to indicate a secure connection. This visual cue helps confirm that your connection is encrypted and that your data is being transmitted safely.

DATA EXCHANGE

Messaging and Calling Applications

Several messaging apps offer robust security systems and use end-to-end encryption to ensure safe communication. Here are some commonly used options:

Signal - A messaging app known for its high level of security and privacy. Signal uses end-to-end encryption to secure messages and also offers features such as self-destructing messages, file sharing, and encrypted voice calls.



WhatsApp - One of the most widely used messaging apps globally. It allows users to send text, voice, and video messages, share files, and make internet-based calls. WhatsApp uses end-to-end encryption, but because it is owned by Facebook (Meta), concerns have been raised about data privacy and metadata collection.

Telegram - A messaging app often compared to WhatsApp. Telegram offers unique features such as group chats with up to 200,000 members, file sharing up to 2 GB, and self-destructing messages. While Telegram supports end-to-end encryption for its “Secret Chats,” its standard chats are not end-to-end encrypted by default. It is also not fully open source, raising transparency concerns.

Wire - A secure messaging app known for its transparency, strong privacy policies, and open-source code. Wire uses end-to-end encryption for messages, as well as voice and video calls. It supports file sharing and group chats with up to 10,000 participants. Wire stands out for its commitment to data protection and openly communicates how user data is collected, stored, and shared.

Important: Always download messaging apps - and any other apps for your phone - only from official sources such as the Google Play Store or Apple App Store to reduce the risk of malware or compromised software.

Secure Email Communication

Email remains one of the most commonly used forms of online communication. However, it can be vulnerable, as messages can be intercepted and read by unauthorized parties. Fortunately, there are several tools and practices that can help you send emails more securely:

- **Pretty Good Privacy** (PGP) - A well-established encryption program that allows you to send and receive encrypted emails securely.
- **ProtonMail** - A free and secure email service that provides end-to-end encryption, ensuring that only the intended recipient can decrypt and read the message.

Phishing - a type of cyberattack where a malicious actor sends an email or message containing a fake link or attachment designed to look legitimate. If clicked, these can expose your device and data to hackers. Always verify the sender's email address before responding or clicking on any links, especially if the message asks you to confirm information or log in to an account.

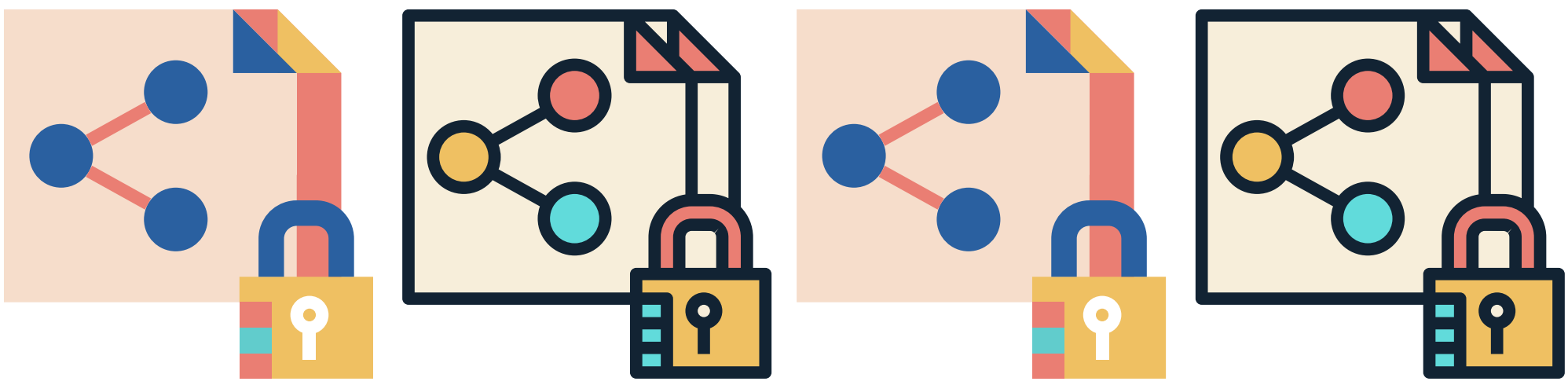
Secure File Sharing

When sharing sensitive files, it's essential to use secure file-sharing services that protect your data from unauthorized access. Avoid sending confidential documents through unencrypted email or over social media.

If you receive a suspicious document by email, **do not download it directly to your device**. Instead, open it in a safe environment using **Google Drive**, **Office 365 online** (not desktop apps), or consider using a tool like **Dangerzone**, which helps safely open potentially risky files.

For even higher levels of privacy and security when sharing files, consider using: **OnionShare** or **SecureDrop**

OnionShare is a tool that allows you to share files and messages anonymously over the TOR network while SecureDrop is a secure platform designed to facilitate safe and anonymous communication between sources and journalists. Both tools offer strong encryption and are built to protect users' identities and encourage the free and safe exchange of sensitive information.



AND MORE...

Privacy on Social Media

This topic can be quite tricky for some journalists. On one hand, journalists are expected to maintain a presence on social media, but on the other hand, they are often criticized for security risks. So, should you hide or be visible across all social networks? There is no one-size-fits-all answer – it depends on the type of work you do and your need as a public media figure to be visible and represented on social media.

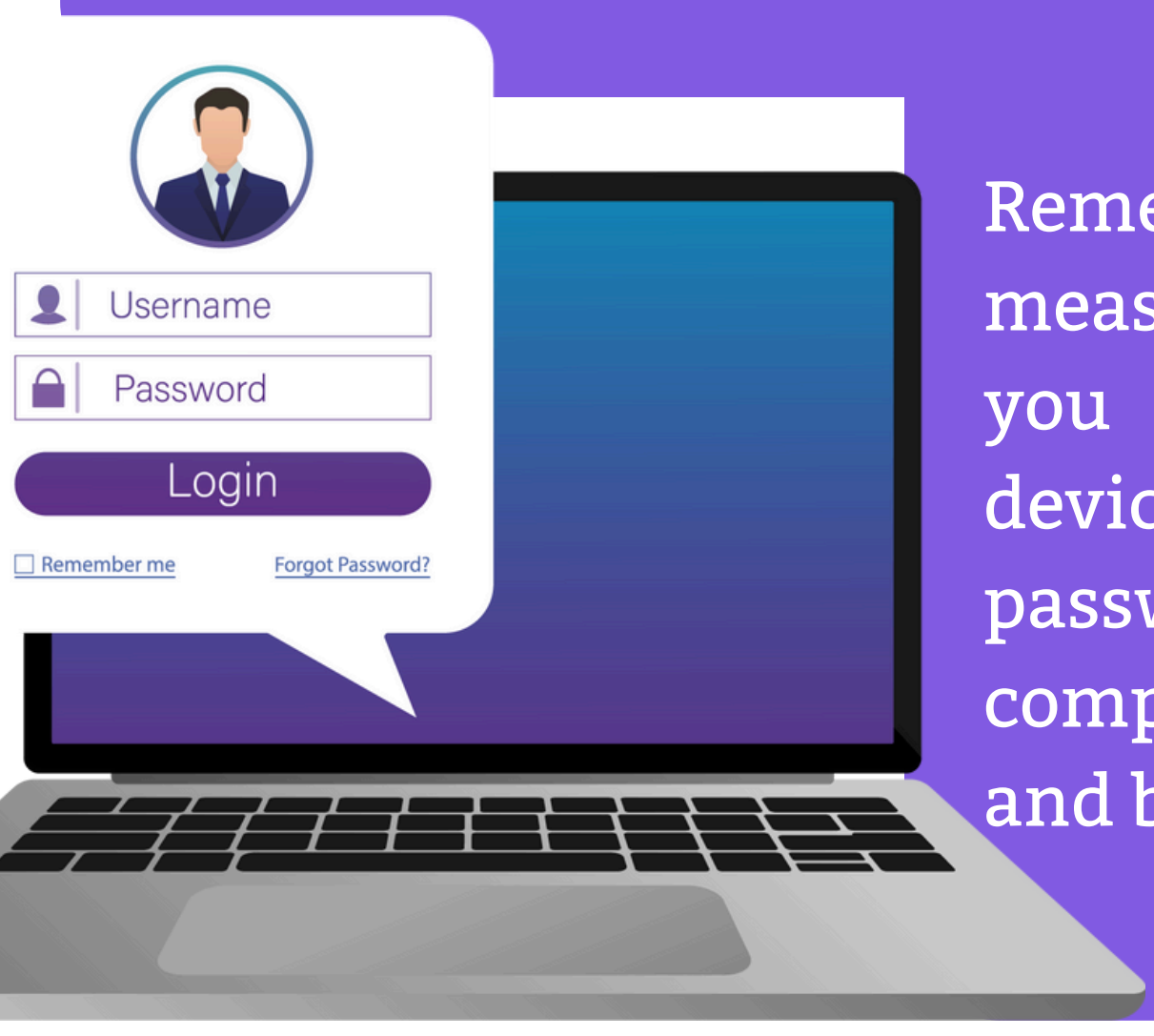
Pay attention to privacy settings on social platforms. Consider whether you should have two separate profiles – one public and one private. Be cautious about sharing personal information, and avoid posting sensitive details like addresses, phone numbers, or other private data. Ensure that your profile is set to private, so only people you choose can see your posts. Additionally, avoid sharing confidential information or documents via social media.

Education

Education is key to online security. It’s essential to continuously educate yourself on emerging threats and how to protect yourself from them. There are numerous free online resources available to help you learn more about online security.

Regular Software Updates

Keep the software on your computer and mobile devices regularly updated to ensure you have the latest security protections. Updates often include patches for security vulnerabilities and improvements in protection.



Device Security

Remember that all security measures are only effective if you physically secure your devices. Always use a password to access your computer or mobile phone and be mindful of where you leave your devices.

ARE YOU FOLLOWING THESE SECURITY MEASURES IN YOUR WORK?

Compiled by Monika Kutri

Zagreb, May 2023.