EBU
OPERATING EUROVISION AND EURORADIO

R 162

SECURITY AND PRIVACY IN SOCIAL MEDIA APPLICATIONS

RECOMMENDATION

Version 1.0

Geneva
December 2023

Document History

EBU Committee	TC	
Drafting Group	Media Cybersecurity Group	
First published	December 2023	
Revised		

Publication Keywords: Social Media, CyberSecurity, Applications, Data Privacy.

Acknowledgement

EBU technical publications are the work of experts from EBU Members, Associate Members and third parties consisting of international standards bodies, industry partners, academic institutions and independent consultants.

Their contribution to EBU technical publications is a very generous act by the individuals concerned and by their employers. The EBU appreciates their efforts and thanks them most sincerely.

This report has been produced with the assistance of the following entities:

EBU Members: MCS group

EBU Project Manager: Lucille Verbaere.

Definitions

Social Media Social Media refers to a variety of technologies that facilitate the sharing of ideas and information among their users. Examples include Facebook, Instagram, X (formerly Twitter) and YouTube. (*Source: Investopedia*)

Application (App) Application, shortened to "App" has become to refer to program applications for mobile devices such as smartphones and tablets. More recently, the shortened version is used for desktop application software as well. (*Source: Wikipedia*)

Data collection: /harvesting: The process of extracting valuable data from a source. The data can be used for various purposes, such as marketing or research, but can also be used maliciously by third parties to compromise the user’s security and privacy. (*Source: Parsehub*)

Device: IT-based hardware such as desktop and laptop computers, smart phones and tablets.

Operating System: (OS) System software that manages IT hardware and software resources and provides common services for device programs. (*Source: Wikipedia*)

Corporate Device: A Device owned and completely managed by the corporation (Media company)

Personal Device: A privately owned Device that can access some corporate IT systems. It is often subject to some form of corporate Mobile Device Management to mitigate security risks.

MFA: Multi Factor Authentication

Security and Privacy in Social Media Applications

Recommendation

The EBU, considering that:

1. Media companies extensively use Social Media Apps for editorial and marketing purposes, using corporate and/or personal accounts and Devices.
2. Social Media Apps and their in-app browsers inherently need access to features and data that may cause data privacy issues.
3. Consent management on Social Media Apps is complex and employees often don't realize what data is collected/harvested.
4. Some data collected by Social Media Apps may put employee safety at risk in the case of a data breach being performed on their systems.
5. The Operating Systems of Devices are nevertheless increasingly performing access controls that successfully block some permissions by default.

Recommends that Media Companies:

1. Use EBU Rec 143: "Cybersecurity Recommendation for Media Vendors' Systems, Software and Services" when purchasing new products and services.
2. Limit the use of Social Media Apps to employees who really need them in their work.
3. Only install Social Media Apps with the highest security and privacy risks on dedicated corporate Devices that are disconnected from the corporate IT environment.
4. Establish clear ownership of a Corporate Device when it is shared by a team. Nominate an employee in the team who is responsible for the Device.
5. Install the latest version of the Devices' Operating Systems as soon as they are released.
6. Use Mobile Device Management for centrally provisioning and managing Devices, their software, and User Access.
7. Thoroughly manage credentials and use strong passwords and MFA for corporate Social Media accounts. Include controls in the publishing process.
8. Do not provide phone numbers or e-mails in an App's settings that could link back to employee personal data.
9. Continuously raise the awareness of employees as to what data is shared with third parties by Social Media Apps on their Corporate and Personal Devices. Make sure they do not use in-app browsers but only OS's default web browsers.
10. Train employees on how to configure privacy settings properly. Make sure they grant permission to Apps on their Corporate and Personal Devices only when required and that they understand associated risks.
11. Continuously monitor and inform users about the privacy and security risks of using Social Media Apps.