חברות וחברי אקדמיה יקרים, מפיקים ויוצרים,

המסמך הבא מפרט את הדרכים בהן אנו מגנים על הנכסים היקרים לכם - הסרטים, מפני פיראטיות באינטרנט.

מטרת המסמך היא לטעת תחושת ביטחון בכל הנוגע לנוכחות של הסרטים באופן מקוון (און ליין).
ברור לנו כי באופן טבעי הרוב מעדיפים הקרנות ומפגשים פנים אל פנים. הזמינות המקוונת לסרטים נועדה להשלים צורך זה ולספק מענה במקרה בו לא מצליחים להגיע לקהל נרחב מספיק.

למי יש גישה לסרטים

- החל מהשנה, אין צורך לשלוח אלינו קבצים. תוכלו להעלות את קבצי הסרטים ישירות למערכת ההקרנות דרך קישור שישלח אליכם בימים שלאחר הרשמתכם לתחרות. המערכת מצפינה אותם אוטומטית, כך שאיש מצוות האקדמיה לא יוכל להוריד אותם.
- מערכת הניהול אינה זמינה ליותר משלושה אנשים. היא גם כוללת רישום פעולות מסודר (לוג), המאפשר לראות איזה מהמשתמשים בעלי הרשאת הניהול ביצע איזו פעולה.
- הסרטים מוצפנים מיד עם העלאתם כאמור. המשמעות היא שגם אם הקובץ הורד, לא ניתן לנגן אותו ומי שמנסה לעשות זאת, יקבל מסך מעורבל.
- כמו בשנה שעברה, כל מסך מכיל בתוכו את מייל המשתמש כסימן מים. זאת כדי למנוע הקלטת מסך (ואם בכל זאת הקלטה כזו נעשה, יש ראיות).
- היחידים שיכולים לגשת לאתר הצפייה עצמו כצופים הם חברות וחברי אקדמיה הרשומים כחברים משלמים ופעילים בימי התחרות. המערכת אינה מאפשרת רישום עבור מי שאינו חבר אקדמיה פעיל.

זמינות הסרטים
זמינות הסרטים שאתם מעלים לתחרות נקבעת על ידכם. כלומר, לא מדובר ב"נגעת - נסעת". גם אחרי שהסרט הועלה לשרת התחרות, תוכלו לתאם איתנו את מועדי זמינותו לחברות וחברי האקדמיה.

דרכי ההגנה על הסרטים
הסרטים כאמור מוצפנים באמצעות מערכת Movies Everywhere. הסבר טכני מפורט על תהליך ההצפנה והדרך בה אנחנו מגנים על הסרטים מצורפת בהמשך. המסמך באנגלית.

Copyright Protection in Movies Everywhere

Being founded by filmmakers, Movies Everywhere considers copyright protection to be of paramount importance. We developed and use our own method, based on known technologies, which were integrated by us to an independent system:

1. The first stage is encoding the film. Once the movie file is uploaded, we convert it and create many small files ("chunks" or segments) whereby each one is encrypted, using HLS AES encryption.
2. AES encryption was adopted by the US government and is also used by other DRM systems such as Microsoft Playready and Google's Widevine.
3. To decrypt those files, a key is needed. We use rotating keys, which are stored on a separate server. Each key can decrypt only one video segment, so finding one key would not provide access to the others.
4. However, it is not enough to encrypt those files, as there is one specific file (index, or manifest file, m3u8) which reads them all upon playback. Without the manifest file, which serves as index, the different video chunks are just a chaotic stack of files, with no playback order. The manifest file arranges them. But the manifest file is accessible to all...
5. In order to solve that, we must "encrypt the decrypter", which is - the place which holds the key to those encrypted files. It is part of the manifest (index file).
6. That manifest file must be open and accessible to the video player which runs the movie. Otherwise, playback would never be possible. So in principle, any hacker who has access to the player (which is also accessible), can theoretically have access to the manifest file. That is a sensitive point.
7. That is why we place a "wall" between the tplayer and the keys is the manifest file. To pass that wall, an authentication key must be provided, before the decryption key is returned. If that authentication succeeds, the key to the encrypted files is given and movie payback is made possible. We know that authentication should be given only to our player, in a session (user's visit) which is legitimate and only during that session (screening time). If the request would come from another source, it will be refused.
8. And how does the player know how to send the right request to the manifest file, if that request code (key) is changing all the time, as mentioned in #2?
9. For that, we use a "dictionary". The manifest file knows what kind of request was submitted according to a pre-written dictionary, which exists both on the player and the server which holds the manifest key.
10. Does it mean that the dictionary is uncrackable? - No. But it requires a lot of effort, to "listen" to enough communication between a manifest file and a player and then gradually interpret the meaning of the entries in that dictionary, like a person learning a new language (interpretation that comes from accumulated context).
11. And since we use this method only internally and not sell it, there is a smaller chance that hackers will have the opportunity to crack it (i.e - have enough time to 'listen' to that communication).

12. In iOS devices, the situation slightly differs. That is because Apple forces the use of its own players. Therefore, although the files are encrypted, the access to the manifest files can be done by an advanced user. However, Apple downloading of source files is not trivial with Apple's player and OS.
13. It is also important to mention that ANY encryption can be cracked. It's just a matter of the effort required. We make it hard enough.
14. Geo-blocking: Our system allows blocking users coming from designated IP addresses based on their geographical location (according to IANA).
15. We are trusted by Oscar® qualifying bodies such as Animest Film Festival and The Israel Academy for Film and Television, as well other international film festivals, cinemas and film institutions