

MPC-3628/MPC-3626

Предпазни мерки за сигурност

Този Помощен наръчник описва предпазните мерки за сигурност при прехвърляне на файлове и стрийминг чрез уреда.

[Предпазни мерки за сигурност](#)[Предпазни мерки при връзка с интернет](#)[Предпазни мерки, свързани с мрежовата функция](#)[Предпазни мерки, свързани с безжичната локална мрежа \(LAN\)](#)

## Предпазни мерки за сигурност

---

Тази тема описва предпазните мерки при свързване на уреда към мрежа.

- Съдържанието на комуникацията може да бъде неусетно прихванато от неоторизирани трети страни в обсега на сигналите. Когато използвате безжична LAN комуникация прилагайте внимателно мерките за сигурност, за да защитите съдържанието ѝ.
- **SONY НЕ НОСИ ОТГОВОРНОСТ ЗА ЩЕТИ ОТ КАКЪВТО И ДА Е ВИД, ПРОИЗТИЧАЩИ ОТ НЕСПАЗВАНЕТО НА ПРАВИЛНИ МЕРКИ ЗА СИГУРНОСТ НА ПРЕДАВАТЕЛНИТЕ УСТРОЙСТВА, НЕИЗБЕЖНОТО ИЗТИЧАНЕ НА ДАННИ, В РЕЗУЛТАТ ОТ СПЕЦИФИКАЦИИТЕ ЗА ПРЕДАВАНЕ, ИЛИ КАКВИТО И ДА БИЛО ПРОБЛЕМИ СЪС СИГУРНОСТТА.**
- В зависимост от работната среда до уреда може да имат достъп неупълномощени трети лица в мрежата. При свързване на уреда към мрежата се постарайте да се уверите, че мрежата е защитена сигурно.
- Когато свързвате този продукт към мрежа, свържете го чрез система, която предоставя защитна функция, напр. рутер или защитна стена. Ако е свързан без такава защита, може да възникнат проблеми, свързани със сигурността.

TP1002273716

## Предпазни мерки при връзка с интернет

---

Тази тема описва предпазните мерки при свързване на уреда към интернет.

- Уредът не може да се свързва чрез безжична LAN мрежа с точка за достъп, която използва единствено WEP или WPA, методи с уязвимости.
- Уредът не е мрежово устройство (например рутер или мрежов комуникатор). Силно се препоръчва да свържете устройството към мрежа, където можете да конфигурирате и управлявате мрежовите настройки по подходящ начин, за да се предпазите от мрежови атаки, като например DoS атаки (атаки за отказ на услуга).
- Когато свързвате уреда към мрежа, свържете го чрез рутер, който е настроен и управляван по подходящ начин или го свържете към LAN порт, който извършва същите функции. Ако бъде свързан без подобна защита (например чрез Wi-Fi мрежа със свободен достъп), може да настъпят проблеми със сигурността. Когато са правилно конфигурирани, рутерите предоставят достатъчна защита срещу DoS атаки или загуба на функционалност на устройствата в мрежата. Ако забележите нещо необичайно, незабавно прекратете връзката на камерата с мрежата.

TP1002273717

## Предпазни мерки, свързани с мрежовата функция

Тази тема описва предпазните мерки относно мрежовата функция на уреда.

- Ако бъде засечен неоторизиран достъп, камерата може да спре да приема комуникации. Ако това се случи, свържете се отново отначало.
- Информацията за удостоверяване за свързване на уреда се показва, когато използвате [Technical] – [Network] – [Wireless] – [SSID] и [Password] в пълното меню. Уверете се, че екранът не може да се вижда от други хора.
- Когато използвате мрежовата функция за първи път, настройката [Technical] – [Authentication] – [Password] в пълното меню е празна. Ако паролата не е конфигурирана, елементите [Network] в менюто за настройки са деактивирани (изобразени в сив цвят) и мрежовите настройки не могат да бъдат конфигурирани.
- Използвайте базово удостоверяване за удостоверяване на достъпа до уреда. Съществува риск от прихващане на комуникациите, освен ако не се осъществявате достъп директно с уреда (без да се свързвате чрез точка за достъп или мрежов хъб) или не използвате режим на мрежов клиент. Sony няма да носи отговорност за щети, получени в резултат от невзети мерки за сигурност, или за проблеми със сигурността, възникнали поради неизбежни обстоятелства, свързани с връзката.
- Когато настройвате потребителското име и паролата си, се уверете, че настройките не са видими за някой друг. Задайте потребителското име и паролата както следва.

[User Name]	<ul style="list-style-type: none"> <li>– Задайте потребителско име, което съдържа от 1 до 16 знака.</li> <li>– То е настроено фабрично на "admin" по подразбиране.</li> <li>– Следните символи са валидни за въвеждане. Букви (главни и малки), цифри, символи ( ! % + , - . = _ )</li> </ul>
[Password]	<ul style="list-style-type: none"> <li>– Задайте парола, съдържаща от 8 до 16 знака и поне 1 или повече букви и 1 или повече цифри.</li> <li>– Следните символи са валидни за въвеждане. Букви (главни и малки), цифри, символи ( ! % + , - . = _ )</li> </ul>

## Предпазни мерки, свързани с безжичната локална мрежа (LAN)

---

Тази тема описва предпазните мерки при свързване на уреда чрез безжична LAN мрежа.

- В Помощния наръчник за този уред точките за достъп до безжична LAN мрежа и рутерите за безжична LAN мрежа, които препредават LAN връзки, се наричат “точки за достъп”.
- Поддържа се само методът за сигурност WPA2 (AES).
- Ако се свържете с точка за достъп без настройка за сигурност, може да станете обект на хакерска атака, достъп от злонамерени трети страни или атаки, базирани на уязвимости. Освен ако не е неизбежно, не се препоръчва връзка без каквато и да е настройка за сигурност.
- Настройването на сигурността при безжична LAN мрежа е изключително важно. Sony няма да носи отговорност за щети, получени в резултат от невзети мерки за сигурност, или за проблеми със сигурността, възникнали, поради неизбежни обстоятелства при използването на безжична LAN връзка.

TP1002273719