https://www.digital.bg/kakvo-trqbva-da-znaem-za-dvufaktornata-avtentikaciq-article449311.html:

Какво трябва да знаем за двуфакторната автентикация (digital.bg)

Публикувано на 11.11.2015 00:00 / от Empower

ОТ EMPOWER

11.11.2015 00:00

Съдържание:

Много онлайн услуги предлагат потвърждаване на вашата самоличност в две стъпки или така наречената двуфакторна автентикация. Активирането на тази опция изисква освен въвеждането на вашата парола, въвеждането и на допълнителен код.

Какво е двуфакторната автентикация

Когато влезете в уеб сайт, който предлага двуфакторна автентикация (така наречената '2FA'), ще трябва да въведете допълнителна парола или ПИН. Тази допълнителна парола може да бъде изпратена до мобилното ви устройство, генерирано от определено приложение или специално устройство. Тъй като трябва да имате тези две пароли, за да влезете в профила си, всеки, който се опитва да хакне акаунта ви ще си има доста главоболия.

С нарасналите проблеми на сигурността и възхода на облачното съхраняване на данни, все повече услуги започват да предлагат двуфакторната автентикация. Ето защо, ако използвате услуга за съхранение на важна информация, която предлага двуфакторна автентикация, определено трябва да я разрешите.

Благодарение на How To Geek можем да разберем колко са видовете двойно потвърждение на пароли.

1. Чрез SMS

Много услуги ви позволяват да влезете в профила си само след като сте въвели код, който сте получили като SMS съобщение всеки път, когато се опитате да се логнете. Този код може да се използва само веднъж. По този начин само този, който знае паролата ви и има достъп до вашия телефон може да влезе в акаунта ви. Това е удобно, тъй като не е нужно да правите нищо специално и повечето хора имат мобилни телефони. Все пак, този метод е зависим от клетъчната мрежа и ако сте някъде, без сигнал, например, няма да можете да получите тези съобщения.

2. Чрез приложение за генериране на код

Има и приложения, които могат да генерират временни кодове. Най-популярното сред тях е Google Authenticator, което Google предлага за Android и iPhone. Инсталирайте приложението, сканирайте кода при създаване на нов акаунт и приложението ще генерира нови кодове на всеки 30 секунди. Ще трябва да въведете текущия код, показан в приложението на телефона ви, както и паролата си, когато искате да се логнете в някой акаунт. Хубавото е, че приложението ще продължи да генерира кодове, дори и без връзка с интернет.

3. Чрез физически ключ

Това е друга опция, която постепенно започва да набира популярност. Големите компании са създали стандарт, известен като U2F, благодарение на който вече е възможно да се използва физически U2F ключ за достъп до профилите ни в Google, Dropbox и GitHub. Това е малко USB устройство, което може да поставите на вашия ключодържател. Всеки път, когато искате да влезете в профила си от нов компютър, ще трябва да поставите USB ключа и да натиснете бутона върху него. Това е всичко, няма нужда да въвеждате никакви кодове. В бъдеще, тези устройства трябва да работят с NFC и Bluetooth за връзка с мобилните устройства, без да има нужда от USB портове.

4. Чрез имейл

Други услуги разчитат на вашия имейл акаунт, за да се уверят, че вие сте истинския притежател на съответния акаунт. Когато се опитате да влезете в някой ваш акаунт от друг компютър, ще трябва да въведете кода за еднократна употреба изпратен до вашия имейл акаунт.

Вижте как да си гарантирате по-голяма сигурност в Интернет:

Как да си гарантирате по-голяма сигурност в Интернет

Публикувано на 27.01.2015 00:10 / от Empower

Пълната анонимност в наши дни е почти невъзможна. И все пак експертите смятат, че има какво да направим по въпроса. Те дават съвети и препоръчват употребата на инструменти, които гарантират сигурността ни.

Ако искате да запазите неприкосновеността на личния си живот, вижте списъка на CIO с продуктите, които гарантират сигурността ни в интернет. И тъй като темата за сигурността в интернет е актуална, още полезни съвети може да намерите в статията 8 полезни съвета за сигурност в Интернет, които е добре да знаем.

И тъй като облачните услуги днес се харесват най-много е добре да се научите как да предпазвате личните си данни. Тук може да намерите повече информация за най-сигурните облачни услуги за съхранение на данни.

1. Hotspot Shield

Hotspot Shield е софтуер, който осигурява безопасно и анонимно сърфиране в мрежата и е на разположение за Mac, Windows, iPhone/iPAD и Android устройства. Hotspot Shield създава криптиран тунел между компютъра и сървърите на доставчика, като по този начин потребителите могат да извършват дейностите си в мрежата анонимно. Софтуерът предоставя възможност за автоматично криптиране на входните и изходните данни.

2. Abine Blur

Abine Blur позволява на потребителите да защитават своите пароли, онлайн плащания и лична информация на всяко устройство. Abine Blur се интегрира с всички браузъри и спира проследяването или предоставянето на лична информация като имейл, телефонен номер или номера на кредитни карти.

3. Places by Ansamb

Places by Ansamb е платформа за безопасно споделяне на файлове и съобщения, чиито бета тестове започнаха през месец януари 2015 година. Тя е достъпна за Linux, Apple OS X и Windows и осигурява автоматично криптиране на видео разговорите на най-високо ниво.

4. OX Guard

OX Guard е инструмент гарантиращ сигурността на електронната ви поща. Той е проектиран така че да ви предложи лесен начин за криптиране на данни и комуникацията ви без да е необходимо предварително да познавате процедурите или техниките на криптографията. OX Guard ви предпазва от неоторизиран достъп до електронната поща и файловете ви по време на съхранението и доставката им на други доставчици на електронна поща.

5. Tor

Първоначално проектиран, изпълнен и въведен като проект за Военноморската изследователска лаборатория на САЩ, днес Tor се използва за различни цели от физическите лица, журналисти, служители на реда и други. Браузърът Tor може да бъде изтеглен напълно безплатно от потребителите. Той има и версия за Android смартфони.

6. The Guardian Project

Докато смартфоните са предвестник на следващото поколение устройства за комуникация, те са една крачка назад, когато става въпрос за личната ни сигурност, анонимност и неприкосновеност на личния живот. The Guardian Project създава лесни за използване сигурни приложения, софтуерни библиотеки с отворен код, както и персонализирани мобилни устройства, които могат да се използват по целия свят от всеки, който търси начини да защити своите комуникации и лични данни.