

OUCH!

В ТОЗИ БРОЙ...

- Пароли
- Какво е удостоверяване в две стъпки
- Как работи

Заключете входа

Преглед

Процесът на удостоверяване, или доказване на това кой сте, е ключов за защитаването на информацията ви – електронна поща, социални мрежи или банкови сметки.

Може и да не знаете, но има три различни начина да докажете кой сте; чрез това, което знаете – като например парола, това, което имате – като например шофьорска книжка, и някаква част от вас самите –

например пръстов отпечатък. Всеки един от тези методи има предимства и недостатъци. Най-разпространеният метод за удостоверяване е този чрез парола, нещо което знаете. За съжаление, използването само на пароли става се по-малко сигурно. В този бюлетин ще ви научим как да се защитите и да заключите входа с нещо далеч по-добро от просто парола, наречено удостоверяване в две стъпки.

Гост-редактор

Тифани Шьонике е директорът по кампании и инициативи в National Cyber Security Alliance (@staysafeonline). През 2016, г-ца Шьонике е работила с Белия дом, правителството и индустрията по разработването и въвеждането на Заклучи Входа, кампания базирана на принципа STOP. THINK. CONNECT.™ относно удостоверяване в две стъпки.

Паролите вече не са достатъчни

Паролите доказват кой сте на базата на нещо, което знаете. Ако обаче някой отгатне или придобие паролата ви, той ще получи достъп до всичката ви информация. Компрометираните пароли са основната причина за хакването на акаунти. Именно затова се говори за ползване на фрази-пароли които са трудни за отгатване, различна парола за всеки акаунт, и никога да не споделяте паролата си с никого. Макар и тези съвети да си остават правилни, паролите вече не са толкова ефективни. За щастие има лесен и бърз начин да контролирате и пазите личната си информация сигурна – нарича се удостоверяване в две стъпки.

Какво е удостоверяване в две стъпки?

Удостоверяването в две стъпки (наричано още проверка в две стъпки, многофакторно удостоверяване, или 2FA) е далеч по-сигурно от просто използването на пароли. То работи чрез изискването на не един, а два различни метода

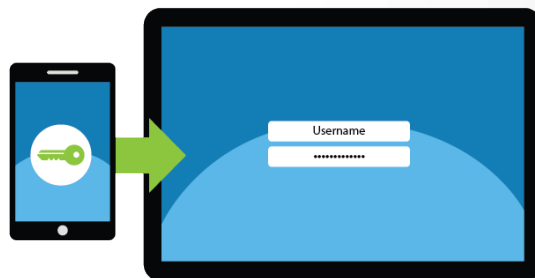
Заклучете входа

да докажете кой сте. Добър пример е банковата ви карта. Когато теглите от банкомат, вие всъщност използвате удостоверяване в две стъпки. За да получите пари в брой, ви трябва две неща – вашата карта (нещо, което имате) и вашият ПИН номер (нещо, което знаете). Ако картата ви бъде изгубена или открадната, никой не може да тегли от вашите пари без да знае ПИН номера. Крадецът трябва да има и картата, и нейният ПИН за да изтегли пари. Удостоверяването в две стъпки използва същата идея.

Как работи

Удостоверяването в две стъпки е широко достъпно за повечето банки, имейл, социални мрежи и други сайтове. В допълнение, повечето от тези сайтове предлагат опростени обяснения как да активирате удостоверяване в две стъпки (за повече информация погледнете ресурсите в края на този бюлетин). Веднъж активирано, удостоверяването в две стъпки би следвало да работи по следният начин. Първо, влизате в акаунта си чрез име и парола, както винаги сте правили. Това е първата от двете стъпки – нещо, което знаете. След това ще получите уникален код, често чрез текстово съобщение на телефона си. След това въведете този код в екрана за влизане. Това е втората от двете стъпки – трябва да имате вашият телефон, за да получите кода. Сега вече акаунта ви е наистина заключен. Дори и ако престъпник ви открадне паролата, той не може да ползва акаунта ви, освен ако нямат и вашият мобилен телефон.

Вместо получаването на кода чрез текстово съобщение, можете да инсталирате специално удостоверително приложение на смартфона си. Това мобилно приложение генерира уникален код всеки път, когато искате да влезете. Предимството на използването на мобилно приложение е, че е още по-сигурно, тъй като кодът е генериран на място от приложението, вместо да се праща като съобщение. В допълнение, това е дори по-удобно, тъй като не е нужно дори да имате мобилен обхват, за да получите код. Приложението постоянно генерира нови кодове, които можете да използвате за достъп до акаунта си.



Заклучете входа чрез удостоверяване в две стъпки където е възможно – това е едно от най-ефективните неща, които можете да направите, за да се защитите онлайн.

Заклучете входа

Дори и в началото удостоверяването в две стъпки да изглежда като повече усилия, личната ви информация ще бъде много по-защитена. Не чакайте, докато акаунта ви бъде хакнат, заключете входа като активирате удостоверяването в две стъпки на най-важните си акаунти, като имейл, банкиране и социални мрежи, и се радвайте на спокойствието от това, че информацията ви е далеч по-сигурна.

НАУЧЕТЕ ПОВЕЧЕ

Абонирайте се за месечния бюлетин за информационна сигурност OUCH!, разгледайте архивните броеве на OUCH! и научете повече за решенията за информационна сигурност на SANS като ни посетите на securingthehuman.sans.org/ouch/archives.

Радослава Несторова (лингвист) и Николай Дачев (технически експерт) са екип, доказал се в областта на техническите преводи. Повече за нас можете да научите на нашите страници в LinkedIn:

<https://www.linkedin.com/pub/radoslava-nestorova/6/6a2/962>

<https://www.linkedin.com/pub/NIKOLAY-DACHEV/7b/5bb/96b>

Ресурси

Пароли-фрази: <https://securingthehuman.sans.org/ouch/2017#april2017>

Сайтове поддържащи 2FA: <https://twofactorauth.org>

Stop|Think|Connect: <https://www.lockdownyourlogin.org>

2FA за Google: <http://www.google.com/landing/2step/>

OUCH! се публикува от SANS Securing The Human и се разпространява под лиценза на [Creative Commons BY-NC-ND 4.0 license](https://creativecommons.org/licenses/by-nc-nd/4.0/). Имате право да разпространявате този бюлетин или да го използвате във вашата информационна кампания, при условие че не го модифицирате. За преводи или повече информация моля пишете на ouch@securingthehuman.org.

Редакторски колектив: Уолт Scrivens, Фил Хофман, Кати Кликнете, Черил Конли
Превод: Николай Дачев и Радослава Несторова



securingthehuman.sans.org/blog



[/securethehuman](https://www.facebook.com/securethehuman)



[@securethehuman](https://twitter.com/securethehuman)



[securingthehuman.sans.org/gplus](https://plus.google.com/securethehuman.sans.org)