ФОНДАЦИЯ
ИНИЦИАТИВА
ЗА ФИНАНСОВА
ГРАМОТНОСТ
www.financialiteracy.eu

50 СЪВЕТА ЗА ВАШАТА ОНЛАЙН ФИНАНСОВА СИГУРНОСТ

Фондация „Инициатива за финансова грамотност“

WWW.FINANCIALITERACY.EU

Автор: Валери Якмаджиев

Живеем все повече във виртуалния свят, но заплахите за нашата сигурност и за нашите пари са напълно реални. Как да се предпазим от финансови измами онлайн е въпрос, който е от ключово значение за всеки от нас. Отговорът може да намерите в съветите, изготвени от експерт по онлайн сигурност, с когото фондация „Инициатива за финансова грамотност“ работи.

КАК ДА СЕ ЗАЩИТИТЕ ОТ ОПАСНОСТИ В ОНЛАЙН ПРОСТРАНСТВОТО?

Пароли:

- ✓ Препоръчително е да се въздържате от употребата на лична информация като собственото име, възраст или дата на раждане, както и тези на близки, роднини или домашни любимци – може да бъде отгатната без особено усилие.
- ✓ Избягвайте употребата на последователни клавиши като qwerty или asdfg.
- ✓ Не ползвайте една и съща парола за всичко.
- ✓ Сменяйте я периодично, например веднъж на 6 месеца.
- ✓ Не е желателно попълването на пароли през публични или чужди устройства, над които нямате контрол.
- ✓ Уверете се, че никой не гледа докато пишете.
- ✓ Винаги заключвайте/разлогвайте устройството си ако го оставяте в присъствие на трети лица – паролата може да бъде откраднатa или сменена само за миг.
- ✓ Не я споделяйте с никого.
- ✓ Използвайте поне 8 знака като включите големи и малки букви, числа и символи, за да усложните отгатването й.
- ✓ Пример за сложна парола, която се помни лесно би бил: Iam:)2b29! , което значи радвам се да съм на 29.
- ✓ Друг лесен за помнене вариант би бил: %tgbHU8* , проследете символите на клавиатурата си – формират латинското V, периодично сменяйте формираната буква, за да промените и паролата си.
- ✓ В случай, на съмнение за изтичане на лична информация, незабавно сменете паролите за достъп до засегнатите ресурси.

- ✓ Ако ползвате софтуерен мениджър за пароли, по-добре да е офлайн.

Обновления (ъпдейти):

- ✓ Винаги прилагайте най-новите обновления за операционната система, тъй като често целта им е да осигурят защита срещу ново-разкрити софтуерни слабости. Настройте график за автоматичното им инсталиране, за да сте сигурни, че не ги пропускате.
- ✓ Същото важи за мобилните устройства, апликациите, които полозвате, както и антивирусните решения.

Анти-вирусен софтуер:

- ✓ Купете, инсталирайте, редовно обновявайте и поддържайте анти-вирусно решение на всяко едно от устройствата, използвани за сърфиране в интернет.
- ✓ Направете график на редовно сканиране за заплахи и следете за изпълненението и резултатите му.
- ✓ Не браузвайте в интернет без защита.
- ✓ Обръщайте внимание на нотификациите от анти-вирусната програма.
- ✓ Следете за нетипично поведение на устройството ви или сайтовете и апликациите, които ползвате.
- ✓ Някои от най-добрите производители включват: Kaspersky, Intel Security (McAfee), Symantec, ESET NOD32, AVG, Sophos, Avira, Avast, bitdefender.
- ✓ Ransomfree by Cybereason безплатно решение за борба с криптиращи вируси.
- ✓ Браузър добавки, които ще ви помогнат в разпознаването на опасни сайтове и файлове, включват: Norton Safe Web, Avast! Online Security, BitDefender TrafficLight. Поддържат се от повечето модерни браузъри.

ФОНДАЦИЯ
ИНИЦИАТИВА
ЗА ФИНАНСОВА
ГРАМОТНОСТ
www.financialiteracy.eu

СИГУРНОСТ ПРИ ОНЛАЙН ПЛАЩАНИЯ

- ✓ Не предоставяйте лична или банкова информация във форми за верификация на акаунт, появили се след, на пръв поглед, неуспешен опит за логване.
- ✓ Ако е възможно отделете устройство за целите на онлайн банкирането и използвайте само него.
- ✓ Алтернативно, ползвайте различен, по-защитен браузър за онлайн банкиране и пазаруване като Epic privacy browser; Comodo Ice Dragon browser; Tor; Dooble; Avira Scout; Microsoft Edge.
- ✓ Не правете каквито и да било финансови транзакции, ако връзката не е сигурна. Това може да бъде лесно проверено с присъствието на **зелено катинарче отляво н а адресът в адресната лента или наличието на префиксът „https“.**
- ✓ Ако е възможно ползвайте кредитна вмето дебитна карта: предимството й е, че по никакъв начин не е обвързана със налична сума в сметката ви.
- ✓ Помислете за употребата на разплащателни портали като PayPal, тъй като в нито един момент по време на транзакцията не въвеждате информация за карти и прочие.
- ✓ Внимавайте с „твърде добри, за да са истина“ оферти.
- ✓ Придържайте се към утвърдени производители с добра репутация.
- ✓ Не правете финансови транзакции, ако сте закачени към публична или незащитена мрежа: много публични мрежи са силно уязвими и лесни за атака. Когато е успешна, извършителят може да инспектира целият потребителски трафик, който минава през мрежата и така да се сдобие с чувствителна информация. Използвайте интернет плана на телефона си.

ЗЛОВРЕДНИ МЕЙЛИ/ЧАТ СЪОБЩЕНИЯ И СОЦИАЛНИ МРЕЖИ

- ✓ Обърнете внимание на обръщението: съобщението адресирано ли е до неясен “Скъп Клиент“ или „Уважаеми госпожи и гспода“? Ако да, бъдете нащрек, компаниите обикновено се обръщат към клиентите си лично.
- ✓ Не издавайте чувствителна информация: банки и легитимни компании не биха изискали от вас информация като номер на кредитна карта по е-мейл.
- ✓ Ако имате друг контакт на лицето, за което отсрещната страна се представя, като различен е-мейл или телефонен номер, свържете се и се уверете, че именно те ви пишат.
- ✓ Гледайте, но не кликайте: задръжте мишката върху бързата връзка и се уверете, че няма разминавания в сайтовете. Ако адресът изглежда странно не го отваряйте.
- ✓ Проверете за правописни грешки: компаниите обикновено се отнасят доста сериозно към е-мейл кореспонденцията. Легитимните бизнеси рядко допускат правописни грешки. Четете внимателно.
- ✓ Бъдете нащрек за заплашителен език и като цяло за създало се усещане за спешност: вменяването му е обичаен фишинг похват, за да ви подтикне към необмислено действие. Не се хващайте на съобщения твърдящи, че акаунтът ви ще бъде изтрит, ако не потвърдите личните си данни, че е имало неоторизиран опит за достъп или че сте прехвърлили лимитът му. Първо проверете фактите.
- ✓ Разгледайте подписа. Липсата на контактна информация на края на писмото може да е индикация за фишинг опит.
- ✓ Не отваряйте прикачени файлове от съмнителни съобщения.
- ✓ Отнасяйте се скептично към нови, непознати последователи или покани за приятелство. Ако случаен човек ви последва или прати покана за приятелство не отговар яйте със същото автоматично . Разгледайте туитовете и постовете му. Препращат ли съдържание, коеото изглежда като спам? Ако да, най-вероятно са ботове, чието приятелство не ви е нужно.
- ✓ Сигнализирайте! Попаднали сте на клип с насилие? Незабавано уведомете отоговорните лица на съответната социална мрежа. Получавате съобщения със странно изглеждащите линкове от ваши приятели? При първа възможност с свържете с тях по алтернативен начин и им кажете за случващото се.

ВНИМАТЕЛНО С МОБИЛНИТЕ УСТРОЙСТВА!

- ✓ Не добавяйте приложения от различни от официалните места за тази цел – google play store или itunes.
- ✓ Обръщайте внимание на правата, които приложенията искат.
- ✓ Въздържайте се от „рутване“ на телефоните си – рутнатите устройства са по-податливи на атаки, а и нарушавате гаранцията им.
- ✓ Поддържайте актуален списък с приложения и махайте всичко ненужно.
- ✓ Инсталирайте анти-вирусен софтуер.
- ✓ Заключвайте екрана.
- ✓ Използвайте апликация за отдалечено изтриване/заключване, в случай, че устройството ви бъде открадното или загубено, например android device manager или iCloud еквивалентът му.