Знаеш ли какво оставяш след себе си онлайн?

Всичко, което правиш в интернет, може да остане там завинаги, дори и след като го изтриеш. Това явление се нарича „цифрово безсмъртие“ и колкото по-рано осъзнаеш как да се пазиш, толкова по-сигурно ще се движиш в дигиталния свят.

Project_YOUth ти помага да бъдеш защитен

Освен че предлага бързи и модерни начини за плащане, Project_YOUth by Postbank има мисия да те информира и защити. В дигиталната ера знанието е най-силната защита.
Най-важното е да внимаваш каква лична информация споделяш онлайн. Не е нужно непознати хора да знаят къде живееш, как се казваш или какъв е телефонният ти номер.

Как да пазиш личните си данни?

Избери силни и различни пароли за всеки свой акаунт – такива, които включват главни и малки букви, цифри и специални символи. Не забравяй и да активираш двуфакторна верификация – тя действа като втори ключ за профилите ти.
Софтуерът на телефона и компютъра ти трябва редовно да се обновява – това не е просто досадно известие, а важна защита срещу пробиви в сигурността. Също така внимавай какви приложения теглиш и откъде. Ако не си сигурен в източника, по-добре не рискувай.

Бъди бдителен, когато си онлайн

Следи какво се случва в профилите ти. Ако нещо изглежда странно – получаваш имейли, за които не си се регистрирал, или виждаш активност, която не си инициирал – това може да е знак, че някой друг има достъп до данните ти.
Когато видиш банер с бутона „Приемам всички“, не бързай. Провери дали можеш да откажеш някои от бисквитките, които събират лична информация за теб. Освен това винаги си струва да прочетеш условията за поверителност – може да са написани сложно, но ако не разбираш нещо, попитай родител или друг възрастен.

Как да разпознаеш фишинг атака?

Фишинг атаката е опит да бъдеш измамен – обикновено чрез имейл или съобщение, което изглежда като изпратено от банка или друга официална институция. Подателите често използват адреси, които приличат на реални, но съдържат малки разлики. В съобщението може да има правописни грешки, неочаквани прикачени файлове или линкове, които водят към съмнителни сайтове.
Задръж курсора върху линка, преди да кликнеш – така ще видиш реалния адрес. Ако той не започва с „https://“ или няма катинарче до него, по-добре не го отваряй. И най-важното – никога не споделяй пароли, ПИН кодове или номера на карти, освен ако не си напълно сигурен, че говориш с официален представител.

YOUth Mode On

Wi-Fi също крие опасности

Безплатните и отворени мрежи може да изглеждат удобни, но често са рискови. Хакери, които използват същата мрежа, могат да откраднат данните ти или дори да поемат контрол над устройството ти. Винаги избирай защитени Wi-Fi мрежи и избягвай да извършваш важни действия през публичен интернет.

Какво да направиш при съмнение за измама?

Ако усетиш, че нещо не е наред – например получиш странен имейл или забележиш необичайни движения по картата си – не се колебай, а веднага се свържи с банката. По-добре да реагираш навреме, отколкото да решаваш проблеми по-късно.

И накрая – запомни това:

Контролът е в твоите ръце. Това, което споделяш онлайн, не е просто информация – това си ти. Бъди разумен, любопитен и информиран. И знай, че Project_YOUth by Postbank е до теб – не само за да плащаш бързо, но и за да живееш дигитално и сигурно.