Препоръки за сигурност за достъп до уеб приложенията на ПОК Доверие

Спазвайки тези препоръки, потребителите на интернет могат да допринесат за по-голяма сигурност на електронните услуги.
Препоръките са групирани в три секции отнасящи се до това какви устройства и системи се използват, как да се работи безопасно и за какво да се проверява и следи в записи и логове на устройствата и системите.

СИГУРНОСТ НА СИСТЕМАТА

1. БЕЗОПАСНИ УСТРОЙСТВА
Уверете се, че устройството, от което достъпвате Моето Доверие се използва само от хора, на които имате доверие или се използва само от Вас. Никога не достъпвайте приложенията на ПОК Доверие от необезопасени устройства, като киоски, обществени и непроверени мрежи или публични компютри.
2. АКТУАЛЗИРАНИ ОПЕРАЦИОНИ СИСТЕМИ И БРАУЗЕРИ
Използвайте само правилно поддържани и обслужвани устройства - операционната система трябва да бъде инсталирана с най-новите актуализации на софтуер за сигурност. Същото важи и за вашия интернет браузър. Активирайте автоматичните актуализации, включително и фишинг и уеб филтъра в браузъра Ви. За повече подробности се обърнете към Вашия администратор или доставчик на софтуерни услуги.
3. ЗАЩИТА СРЕЩУ ВИРУСИ
Използвайте актуална програма за защита от вируси с редовни автоматични актуализации срещу шпионски софтуер, вируси, троянски коне и/или активирайте лична защитна стена, за да защитите устройството си.

БЕЗОПАСНО ПОВЕДЕНИЕ

4. ПОВЕРИТЕЛНОСТ НА ПОТРЕБИТЕЛСКО ИМЕ И ПАРОЛА
Никога не предавайте личните си данни за достъп и оторизация, като например парола, ПИН или код за КУКЕП (Квалифицирано удостоверение за квалифициран електронен подпис), на трети страни и ги въвеждайте само на проверената интернет страница на ПОК Доверие, в която имате индивидуални осигурителни партиди. Никога не ги въвеждайте в имейли, формуляри или непознати системи за онлайн услуги.
5. ВИНАГИ ВЪВЕЖДАЙТЕ ЦЕЛИЯ ИНТЕРНЕТ АДРЕС НА ПОК ДОВЕРИЕ РЪЧНО
Никога не следвайте хипервръзки в електронна поща или други уебсайтове на (предполагаемия) портал за онлайн услуги на ПОК Доверие. Много често това се използва от така наречените „фишинг“ атаки, при които се изисква да потвърдите акаунта си в сайт, приличащ на истинския.
6. ПРОВЕРЯВАЙТЕ ЗАРЕДЕНИЯ САЙТ И АТРИБУТИ ЗА СИГУРНОСТ
Прочетете внимателно адреса на онлайн услугите на ПОК Доверие и го запомнете, за да го разпознаете при следващото влизане. Уверете се, че връзката е защитена и криптирана. Направете това, като проверите дали можете да видите символ за заключване и префикса „***https://...***“, показан в адресната лента на браузъра. Ако

подозирате, че връзката е несигурна, проверете също дали шифроването е разрешено с помощта на цифров сертификат за сигурност. За да направите това, щракнете върху символа за заключване в браузъра си, за да проверите автентичността на сертификата за сигурност. Ако в адресната лента се покаже само префиксът „***http://...***“, това определено не е легитимна интернет страница на ПОК Доверие.

7. НЕ СЪХРАНЯВАЙТЕ ПОТРЕБИТЕЛСКОТО ИМЕ И ПАРОЛА НА ВАШИЯ КОМПЮТЪР

Пазете вашата поверителна онлайн информация на сигурно място. Тъй като данните на компютъра могат да бъдат проследявани, ние ви съветваме да не ги съхранявате на Вашия компютър.

ВЪЗМОЖНИ ОПАСНОСТИ

8. НАЛИЧИЕ НА НЕПОЗНАТИ ЗА ВАС ОПЕРАЦИИ

ПОК Доверие не изпраща електронни писма с молба към клиентите си да разкриват информация за поверителен достъп, данни и операции, като потребителски номер, парола или ПИН за КУКЕП. Ако получите такъв емейл това е сигурен признак за опит за нерегламентиран достъп.

9. НЕПОЗНАТИ IP АДРЕСИ

Проверявайте в записите на онлайн приложението за непознати IP адреси достъпвали Вашата Индивидуална осигурителна партида. За повече информация може да се обърнете към ИТ специалист за идентифициране и проследяване на IP адрес.

10. СТАТУСА НА АНТИВИРУСНИЯ ВИ СОФТУЕР

Редовно проверявайте актуализиран ли е и дали работи антивирусния Ви софтуер. Често срещат ефект от заразяването на компютъра е блокирането работата на антивирусния софтуер или спиране на обновленията му.