**Рекомендації споживачам ТОВ «Інстафінанс»
щодо негайного інформування про несанкціонований доступ або зміну інформації споживача в системах дистанційного обслуговування ТОВ «Інстафінанс» (далі – Компанія)**

З метою забезпечення високого рівня безпеки інформації та унеможливлення доступу сторонніх осіб до конфіденційної інформації споживачів під час користування системами дистанційного обслуговування Компанії пропонуємо використовувати рекомендації наведені нижче.

Рекомендації щодо безпечного використання систем дистанційного обслуговування Компанії:

☐ Використовуйте надійні паролі для запобігання несанкціонованого доступу до пристроїв з яких Ви здійснюєте доступ до систем дистанційного обслуговування Компанії. Важливо створювати унікальну складну комбінацію для входу до облікового запису.

☐ Для запобігання несанкціонованого доступу до конфіденційної інформації не повідомляйте свої авторизаційні дані у системах дистанційного обслуговування (логін, пароль тощо) третім особам (включаючи членів родини, друзів і т.д.).

☐ При використанні паролів не рекомендується зберігати паролі взагалі, в будь-якому місці (на папері, на комп’ютері, на флеш-носіях, дискетах тощо). Пароль рекомендується запам’ятати.

☐ Компанія ніколи та за жодних обставин не здійснює розсилку електронних листів із вимогою надіслати ключ, логін чи пароль, перейти за вказаною електронною адресою, а також не розповсюджує електронною поштою комп’ютерні програми. Відповідальність за збереження ключів та паролів покладається на користувача.

☐ У разі отримання подібних листів, програм чи будь-яких повідомлень електронною поштою, необхідно терміново проінформувати про це Компанію, зателефонувавши за номером 0(800)50-07-55 або надіслати повідомлення на електронну пошту info@ukrpozyka.com.ua.

☐ Рекомендується видаляти підозрілі електронні листи без їх відкриття, особливо листи від невідомих відправників із прикріпленими файлами, що мають розширення *.exe, *.pif, *.vbs та інші файли.

☐ Звертайте увагу на можливі повідомлення веб-браузера про будь-яку небезпеку. У разі виникнення будь-якої підозри рекомендується завершити роботу із системою дистанційного обслуговування та закрити її.

☐ Не відповідайте на запити (найчастіше запити розсилаються через SMS-повідомлення засобами мобільного зв’язку, електронною поштою тощо), які містять вимогу надати або перевірити логін, пароль тощо.

☐ Уникайте підключення до публічних Інтернет-мереж, які є менш захищеними та часто поширюють різні загрози.

☐ На комп'ютерах, з яких здійснюється робота в системі, використовуйте тільки ліцензійні операційні системи і антивірусні програми з регулярно оновлюваними антивірусними базами. Також регулярно оновлюйте операційну систему (в першу чергу це стосується оновлень безпеки). У повсякденній роботі не використовуйте обліковий запис із правами локального адміністратора (використовуйте призначений для користувача обліковий запис).

☐ Нікому не передавати управління своїм Обліковим записом в системі дистанційного обслуговування.

☐ Нікому не передавати в будь-якій формі свої логін та пароль Облікового запису в системі дистанційного обслуговування.

☐ Клієнт має забезпечити захист свого мобільного телефону та SIM-картки, на номер якої система дистанційного обслуговування надсилає коди підтвердження операцій.

☐ Клієнт має забезпечити антивірусну безпеку своїх інформаційних систем (на персональних комп'ютерах, смартфонах, планшетах і т.д.), за допомогою яких виконується доступ до системи дистанційного обслуговування.

☐ Негайно змінити пароль в системі дистанційного обслуговування у випадку якщо пароль, або його частина стала відома іншій особі.

Витяг з Правил надання фінансових послуг ТОВ «Інстафінанс»

«п. 3.6. Якщо пароль від Особистого кабінету стане відомим або може стати відомим третій особі, Позичальник повинен негайно повідомити про це Позикодавця письмово або телефоном, а Позикодавець повинен невідкладно заблокувати доступ до Особистого кабінету, доки, поки на основі заяви Позичальника, не буде надано новий пароль від Особистого кабінету, і Позичальник не надасть вказівку Позикодавцю про розблокування Особистого кабінету.»

Рекомендації щодо дій з негайного інформування Компанії про несанкціонований доступ або зміну інформації споживача в системах дистанційного обслуговування

Максимально швидко звертайтесь до Компанії у разі:

☐ виявлення втрати Картки або підозри на її незаконне використання;

☐ викрадення мобільного телефону з номером телефону, який є фінансовим номером;

☐ несанкціонованого доступу або зміни Вашої інформації в системах дистанційного обслуговування.

Цілодобова клієнтська підтримка: 0(800)50-07-55

Надіслати повідомлення на електронну пошту: info@ukrpozyka.com.ua

Надіслати повідомлення за формою зворотного зв'язку:
https://www.ukrpozyka.com.ua/zvorotnii-zvyazok