

РЕКОМЕНДАЦИИ ПО ВЕДЕНИЮ ОНЛАЙН БЭНКИНГА	EMPFEHLUNG ZUM ONLINE-BANKING
<p>При работе в онлайн банкинге имеет место быть риск воровства или неправомерного использования банковских данных хакерами, в результате шпионажа, физической атаки или обмана.</p> <p>РУФИЛ предпринимает все необходимые меры для предотвращения подобного риска. В первую очередь:</p> <ul style="list-style-type: none"> - применение антивирусных программ и анти-шпионского программного обеспечения. - регулярное обучение сотрудников по вопросам защиты и безопасности данных и - использование двух отдельных электронных ключей доступа. <p>При работе в онлайн банкинге мы рекомендуем каждому клиенту использовать два различных электронных ключа доступа.</p> <ul style="list-style-type: none"> - Административный ключ доступа с ограниченными правами и - ключ полного доступа с полными правами. <p>Сотрудник компании Руфил при этом получает административный ключ доступа с ограниченным доступом к счёту. Таким образом он может подготавливать на подпись в онлайн банкинге перечисления для клиентов. Сотрудник компании Руфил не может активизировать перечисления.</p> <p>Клиент или клиентом уполномоченное лицо получает полный ключ доступа. Он один владеет ключом и данными, прилагаемыми к нему, чтобы иметь возможность осуществления перечислений.</p> <p>Только по настоятельному желанию клиента РУФИЛ берёт на себя работу с полным ключом. В этом случае РУФИЛ по поручению клиента имеет дело с одним из зарегистрированных на клиента ключом и не несёт материальной ответственности, если наносится вред в результате неправомерного использования или воровства банковских данных хакерами, в результате шпионажа, физической атаки, обмана и т. д.</p>	<p>Bei der Arbeit im Online-Banking gibt es das Risiko des Diebstahls oder Missbrauchs von Bankdaten durch Hacker, Spionage, physischen Einbruch oder Betrug.</p> <p>RUFIL CONSULTING trifft alle üblichen Vorkehrungen, um dieses Risiko so gering wie möglich zu halten. Dazu gehören in erster Linie</p> <ul style="list-style-type: none"> - der Einsatz von Anti-Virus und Spyware-Software, - regelmäßige Schulung der Mitarbeiter im Bezug auf Datensicherheit und - die Verwendung zweier getrennter elektronischer Zugangsschlüssel. <p>Wir empfehlen jedem Kunden bei der Arbeit mit dem Online-Banking zwei verschiedene und getrennte elektronische Zugangsschlüssel zu verwenden.</p> <ul style="list-style-type: none"> - Einen administrativen Zugangsschlüssel mit begrenzten Zugriffsrechten und - einen vollen Zugangsschlüssel mit vollen Zugriffsrechten. <p>Der RUFIL Mitarbeiter erhält dabei den administrativen Zugangsschlüssel mit dem begrenzten Zugang zum Konto. So kann er im Online-Banking arbeiten und Überweisungen für den Kunden unterschriftsreif vorbereiten. Der RUFIL Mitarbeiter kann keine Überweisungen freigeben.</p> <p>Der Kunde, bzw. eine vom Kunden dafür autorisierte Person erhält den vollen Zugangsschlüssel. Er allein besitzt den Schlüssel und die dazugehörenden Daten, um Überweisungen tätigen zu können.</p> <p>Nur wenn es der Kunde ausdrücklich anders wünscht, übernimmt RUFIL CONSULTING die Arbeit mit dem vollen Zugangsschlüssel. RUFIL CONSULTING handelt in diesem Fall im Auftrag des Kunden mit einem auf den Kunden registrierten Zugangsschlüssel und übernimmt keine Haftung, wenn durch Missbrauch oder Diebstahl von Bankdaten durch Hacker, Spionage, physischen Einbruch, Betrug o.ä. Schaden entsteht.</p>

