ПромСвязьИнвест
расчетная небанковская кредитная организация
367000 РФ, Республика Дагестан, г. Махачкала, ул. Ирчи-Казака 2 «б»
ОКПО 43340114 БИК № 048209395 корсчет 30103810982090000039 5
тел.(8722) 62-16-24, 61-58-22 факс.(8722) 62-16-94 www.psib.ru E-mail: office@psib.ru

«18» января 2021г. **г. Махачкала**

«Информирование клиентов системы дистанционного банковского обслуживания «iBank2» о мерах защиты за декабрь 2020 г.»

В связи с необходимостью снижения рисков воздействия вредоносного кода, рисков использования уязвимостей программного обеспечения и повышения уровня защиты информации при работе с системой дистанционного банковского обслуживания «iBank2» (Интернет-банком) служба информационной безопасности РНКО «ПРОМСВЯЗЬ ИНВЕСТ» (ООО) рекомендует it-специалистам наших клиентов (организаций и индивидуальных предпринимателей) применять в своей работе рекомендации по защите информации, указанные в Приложениях 1 и 2 к данному письму. В случае возникновения вопросов по применению рекомендаций просим Вас позвонить в службу информационной безопасности по номеру 8 (8722) 51-70-44.

ВРИО Председателя Правления подпись **Исланов М.О.**

М.П.

Исп. Ирганов Ю.Г.
Руководитель СИБ
8 (8722) 62-62-39

Приложение № 1
к информационному письму
«Информирование клиентов системы
дистанционного банковского
обслуживания «iBank2» о мерах
защиты за декабрь 2020 г.»

По информации **ФИНЦЕРТ (центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере, специального структурного подразделения Банка России)** участились случаи распространения вредоносного программного обеспечения семейства «RTM», ориентированного на клиентов кредитно-финансовых организаций, являющихся юридическими лицами и индивидуальными предпринимателями.

URL-адреса и IP-адреса, рекомендуемые к блокировке it-специалистами организаций и индивидуальных предпринимателей через сетевые экраны, брандмауэры, сетевое оборудование	**afonina@nppkant.ru** **45.61.136.191** **167.172.151.128** **165.22.211.203** **45.61.136.241** **avsvmcloud.com** **deftsecurity.com** **freescanonline.com** **thedoccloud.com** **websitetheme.com** **highdatabase.com** **157.245.142.162** **172.86.75.87**

При работе с электронной почтой организациям и индивидуальным предпринимателям следует учитывать, что участились случаи отправки по электронной почте ложных писем от мошенников. Целью данных писем является распространение вредоносного кода с целью кражи денежных средств. Подобные письма содержат файлы со следующими именами:

Электронное требование ФНС.rar
Документы.zip
Электронное требование ФНС.exe
Oplata po kontraktu za proshlyj mesyac.exe
Dannye dlya oformleniya doverennostej za proshlyj mesyac.exe
Sverit' dannye oktyabr'-noyabr'.exe
Proekt dogovora 3e dekabrya.exe
Paket dokumentov 3e dekabrya.exe
Sverit' dannye 03.12.exe
Doverennosti 03.12.exe
Dok-ty za etot mesyac.exe
Dannye dlya doverennosti oktyabr'-noyabr'.exe
Dannye dlya oformleniya doverennostej za proshlyj mesyac.exe
Pasportnye dannye chetverg.exe
Dok-ty 3e dekabrya.exe

При обнаружении во входящих письмах своей электронной почты писем с файлами с подобными именами не рекомендуется открывать такие файлы и такие письма.

На компьютере, с использованием которого осуществляется работа в системе ДБО «iBank2», не рекомендуется устанавливать программное обеспечение, имеющее уязвимости с критичным уровнем опасности. К такому программному обеспечению относится программное обеспечение, указанное в таблице ниже.

№	Наименование уязвимого программного Обеспечения	Идентификатор уязвимостей	Описание уязвимости	Дата выявления	Ссылка на источники	Наличие обновлений
1.	Удаленное выполнение кода в Mozilla Thunderbird	MITRE: CVE-2020-26970	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством подключения пользователя к вредоносному SMTP-серверу. Уязвимость обусловлена некорректной обработкой ответных сообщений от SMTP-сервера.	2 декабря 2020 г.	https://www.cybersecurity-help.cz/vdb/SB2020120213	Есть
2.	Множественные уязвимости в Google Chrome	MITRE: CVE-2020-16037 CVE-2020-16038 CVE-2020-16039	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена ошибкой использования памяти после освобождения в медиакомпонентах.	2 декабря 2020 г.	https://chromereleases.googleblog.com/2020/12/stable-channel-update-for-desktop.html	Есть
3.	Множественные уязвимости в Google Chrome	MITRE: CVE-2020-16040	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена некорректной проверкой входных данных компонентом V8.	2 декабря 2020 г.	https://chromereleases.googleblog.com/2020/12/stable-channel-update-for-desktop.html	Есть
4.	Несанкционированный доступ в продуктах Zyxel	MITRE: CVE-2020-29583	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД и административные привилегии в целевой системе. Уязвимость обусловлена наличием жестко-закодированной учетной записи “zyfwp“ с неизменяемым паролем.	22 декабря 2020 г.	https://www.cybersecurity-help.cz/vdb/SB2020122410 http://ftp.zyxel.com/USG40/firmware/USG40_4.60(AALA.1)C0_2.pdf https://businessforum.zyxel.com/discussion/5252/zld-v4-60-revoke-and-wk48-firmware-release https://businessforum.zyxel.com/discussion/5254/whats-new-for-zld4-60-patch-1-available-on-dec-15 https://www.eyecontrol.nl/blog/undocumented-user-account-in-zyxel-products.html https://www.zyxel.com/support/CVE-2020-29583.shtml https://www.zyxel.com/support/security_advisories.shtml	Есть
5.	Множественные уязвимости в продуктах Mozilla	MITRE: CVE-2020-26974	Эксплуатация уязвимости позволяет удалённому злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально сформированной вредоносной веб-страницы. Уязвимость обусловлена некорректным определением типа CSS-объекта при использовании свойства «flex-	15 декабря 2020 г.	https://www.cybersecurity-help.cz/vdb/SB2020121531 https://www.cybersecurity-help.cz/vdb/SB2020121533	Есть

			basis».			
6.	Множественные уязвимости в продуктах Mozilla	MITRE: CVE-2020-35112	Эксплуатация уязвимости позволяет удалённому злоумышленнику получить НСД к целевой системе посредством открытия пользователем специально созданного вредоносного загруженного файла. Уязвимость обусловлена некорректной обработкой загруженных файлов без расширений.	15 декабря 2020 г.	https://www.cybersecurity-help.cz/vdb/SB2020121531 https://www.cybersecurity-help.cz/vdb/SB2020121533	Есть
7.	Множественные уязвимости в продуктах Mozilla	MITRE: CVE-2020-35113 CVE-2020-35114	Эксплуатация уязвимости позволяет удалённому злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально сформированной вредоносной веб-страницы. Уязвимость обусловлена некорректной обработкой содержимого HTML-страниц.	15 декабря 2020 г.	https://www.cybersecurity-help.cz/vdb/SB2020121531 https://www.cybersecurity-help.cz/vdb/SB2020121533	Есть
8.	Множественные уязвимости в ПО Foxit Reader	MITRE: CVE-2020-13547	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного PDF-файла. Уязвимость обусловлена использованием несовместимых типов в функции openPlayer().	9 декабря 2020 г.	https://talosintelligence.com/vulnerability_reports/TALOS-2020-1171 https://talosintelligence.com/vulnerability_reports/TALOS-2020-1175 https://talosintelligence.com/vulnerability_reports/TALOS-2020-1165 https://talosintelligence.com/vulnerability_reports/TALOS-2020-1166 https://talosintelligence.com/vulnerability_reports/TALOS-2020-1181	Есть
9.	Множественные уязвимости в ПО Foxit Reader	MITRE: CVE-2020-13548	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного PDF-файла или веб-страницы. Уязвимость обусловлена ошибкой использования памяти после освобождения в движке JavaScript.	9 декабря 2020 г.	https://talosintelligence.com/vulnerability_reports/TALOS-2020-1171 https://talosintelligence.com/vulnerability_reports/TALOS-2020-1175 https://talosintelligence.com/vulnerability_reports/TALOS-2020-1165 https://talosintelligence.com/vulnerability_reports/TALOS-2020-1166 https://talosintelligence.com/vulnerability_reports/TALOS-2020-1181	Есть
10.	Множественные уязвимости в ПО Foxit Reader	MITRE: CVE-2020-13570	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного PDF-файла или веб-страницы. Уязвимость обусловлена ошибкой использования памяти после освобождения в движке JavaScript.	9 декабря 2020 г.	https://talosintelligence.com/vulnerability_reports/TALOS-2020-1171 https://talosintelligence.com/vulnerability_reports/TALOS-2020-1175 https://talosintelligence.com/vulnerability_reports/TALOS-2020-1165 https://talosintelligence.com/vulnerability_reports/TALOS-2020-1166 https://talosintelligence.com/vulnerability_reports/TALOS-2020-1181	Есть
11.	Выполнение произвольного кода в Microsoft Office	MITRE: CVE-2020-17124	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного файла. Уязвимость обусловлена некорректной проверкой входных данных.	8 декабря 2020 г.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-17124 https://www.cybersecurity-help.cz/vdb/SB2020120821	Есть
12.	Выполнение произвольного кода в ОС Windows	MITRE: CVE-2020-17096	Эксплуатация уязвимости позволяет удаленному аутентифицированному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированного SMBv2 пакета. Уязвимость обусловлена некорректной проверкой входных данных в драйвере файловой системы Windows NTFS.	8 декабря 2020 г.	https://www.cybersecurity-help.cz/vdb/SB2020120829 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-17096	Есть

13.	Выполнение произвольного кода в ПО Adobe	MITRE: CVE-2020-24440 CVE-2020-24447	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного DLL-файла. Уязвимость обусловлена некорректной загрузкой DLL-библиотек.	8 декабря 2020 г.	https://www.cybersecurity-help.cz/vdb/SB2020120851 https://helpx.adobe.com/security/products/prelude/apsb20-70.html https://helpx.adobe.com/security/products/lightroom/apsb20-74.html	Есть
14.	Удаленное выполнение кода в Microsoft Visual Studio	MITRE: CVE-2020-17156	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия специально сформированного вредоносного файла. Уязвимость обусловлена некорректной проверкой входных данных.	8 декабря 2020 г.	https://www.cybersecurity-help.cz/vdb/SB2020120844 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-17156	Есть
15.	Выполнение произвольных команд в продуктах VMware	MITRE: CVE-2020-4006	Эксплуатация уязвимости позволяет удаленному аутентифицированному злоумышленнику выполнить произвольные команды в целевой системе посредством внедрения специально сформированных команд управления в административной панели. Уязвимость обусловлена некорректной обработкой входных данных при выполнении команд.	3 декабря 2020 г.	https://nvd.nist.gov/vuln/detail/CVE-2020-4006 https://www.vmware.com/security/advisories/VMSA-2020-0027.html	Есть

Приложение № 2
к информационному письму
«Информирование клиентов системы
дистанционного банковского
обслуживания «iBank2» о мерах
защиты за декабрь 2020 г.»

Признаки телефонного мошенничества, способы защиты от телефонного мошенничества.

Мошеннических схем много, и регулярно появляются новые. Чтобы не стать жертвой обмана, полезнее знать не столько сами схемы, сколько ключевые признаки того, что вы столкнулись с мошенником.

По статистике в четырех из пяти случаев мошенничества клиенты банков теряют свои деньги не из-за хакерской атаки, а из-за того, что сами их отдают или сообщают мошенникам реквизиты карт. Обычно мошенники выуживают номер и срок действия карты, трехзначный CVV/CVC-код, а также пароли и коды из СМС, которые банки присылают для подтверждения операций. То есть киберпреступники – это по большей части не столько хакеры, сколько психологи, которые «взламывают» не компьютер (ноутбук, телефон, планшет и другое), а сознание своей жертвы.

По каким же признакам можно распознать мошенников?

1) На вас выходят сами

Кто-то сам вам звонит (пишет письмо, присылает ссылку и так далее). Вне зависимости от того, кем он представляется, – сотрудником банка, полиции, магазина, братом миллионера из Нигерии – и чего он хочет, надо быть осторожным. Помните: если кто-то незнакомый звонит вам, значит ему что-то нужно. Вопрос: что?

2) Разговор касается денег или вашей банковской карты

Важно помнить, что у мошенников единственная цель – ваши деньги. Ключ к ним – банковская карта. Жулики либо вынуждают человека самого отдать деньги, либо выуживают у него информацию (например, данные карты), которая позволит эти деньги украсть. Если вас просят перевести деньги на некий счет, заплатить налог, бронь, штраф, внести залог, аванс или совершить другие действия, связанные с денежным переводом или раскрытием данных карты, – это скорее всего мошенники.

3) Делают супер-выгодное предложение или пугают

Вам делают супер-выгодное предложение: щедрые выплаты, призы, невероятно привлекательные условия по кредитам и депозитам, инвестиционные продукты, обещающие огромную доходность. При этом вас убеждают, что нельзя упускать шанс получить сразу много денег, надо обязательно использовать уникальную возможность. Противоположная схема – вас пытаются запугать: деньги вот-вот украдут, спишут со счета, вы лишитесь потенциального дохода.

Имейте в виду, что у мошенников всегда заготовлены ответы на возможные вопросы. Поэтому даже не пытайтесь вступать с ними в беседу, ведь чем дольше вы беседуете, тем крепче вас «подсаживают на крючок».

Помните, если вам обещают многое, требуя взамен малое, то вы лишитесь либо малого, либо всего, что есть на карте, но так и не получите ничего взамен.

4) Морально давят, требуют принять решение немедленно

Мошенники работают с большим количеством людей. Им некогда долго возиться с каждым в отдельности. Кроме того, их задача – не дать жертве опомниться. Поэтому они всегда требуют от человека быстрого принятия решений, действуют уверенно и агрессивно. Если вы чувствуете, что на вас давят, угрожают, ставят условие сделать покупку, совершить транзакцию «либо сейчас, либо никогда» – прерывайте общение. Это точно мошенники.

5) Запрашивают информацию о банковской карте

Банки обязаны отслеживать подозрительные операции со счетами своих клиентов. Если у банка возникает подозрение, что совершается несанкционированная операция, его представитель может связаться с владельцем счета и уточнить, действительно ли он совершает эту операцию. Владелец счета должен только подтвердить или не подтвердить операцию – на этом общение заканчивается. Мошенники же начинают выуживать разные данные: коды из СМС, номер карты, трехзначный код на ее обратной стороне, ПИН-код и так далее. Важно помнить, что настоящий сотрудник банка никогда и ни при каких обстоятельствах не будет запрашивать у человека данные его карты. Если кто-то пытается это сделать, прервите разговор – вы общаетесь с мошенником.

Если вы будете всегда помнить об этих признаках, то вне зависимости от хитрости и новизны мошеннической схемы, не попадете в расставленные сети. Важно понимать, что каждый из этих признаков в отдельности не является однозначным доказательством того, что с вами говорят мошенники (кроме случаев, когда у вас запрашивают трехзначный код на обратной стороне банковской карты, ПИН-код или код из СМС). Но чем больше таких признаков, тем больше вероятность того, что вас пытаются обмануть.

Если после разговора с незнакомцем у вас возникли какие-то сомнения или вопросы, перезвоните в свой банк по номеру телефона, указанному на его сайте или банковской карте, и уточните интересующую вас информацию.