

Приложение 1 к письму Отделения-
НБ Карачаево-Черкесская Республика
«О направлении материалов по
киберграмотности»

Ссылка и QR-код на информационные видеоролики Банка России по теме профилактики кибермошенничества:

<https://disk.yandex.ru/d/MEwy-ZliXds1KA;>



1. Аналитические данные Банка России за 2023 год -

[http://www.cbr.ru/analytics/ib/operations_survey/2023/;](http://www.cbr.ru/analytics/ib/operations_survey/2023/)



2. Ежеквартальная статистика Банка России -

http://www.cbr.ru/statistics/ib/#a_118726;



3. Ссылка на образовательные материалы, в составе которых
«конструктор» слайдов –

https://finclass.info/_wt/cybergram:



4. Карточки по тематике киберграмотности –

Банк России

ЧТО ДЕЛАТЬ, ЕСЛИ С КАРТЫ УКРАЛИ ДЕНЬГИ?

1 ЗАБЛОКИРОВАТЬ КАРТУ
 Не паникуйте, немедленно позвоните по телефону горячей линии Банка России 8 800 707 10 70 или на сайте www.banki.ru

2 НАЙТИ ДЕНЕЖКУ
 Если вы обнаружили украденную карту, немедленно сообщите об этом в полицию

3 ОБРАТИТЬСЯ В ПОЛИЦИЮ
 Обратитесь в полицию по месту жительства или в отделение полиции по месту совершения преступления

КАК ПРЕДОТВРАТИТЬ ДРУЖИТВО С ФАЙВЕР?

УКОМПЬЮТЕРИТЕ СООБЩАЮЩИХ
 Не сообщайте никому свои данные, логины, пароли, PIN-коды, номера карт, адреса электронной почты, номера телефонов

НЕ ОТКРЫВАЙТЕ
 Не открывайте письма от неизвестных отправителей

УСТАНОВИТЕ
 Установите антивирусное ПО

Важно! Банк не компенсирует суммы, украденные при использовании интернет-банкинга

Федеральная служба по техническому и экспортному контролю

Банк России

ОСТОРОЖНО: ТЕЛЕФОННЫЕ МОШЕННИКИ!

5 ПРИЗНАКОВ ОБМАНА

1 НА ВАС ВЫЗЫВАТ САМИ
 Неизвестный вам человек звонит по телефону и предлагает помощь, кредит, участие в конкурсе, розыгрыше, сообщает о выигрыше, сообщает о проблемах с картой, сообщает о проблемах с доставкой товара

2 НА ВАС ДАВЯТ
 Ассистентка оператора службы поддержки сообщает о проблеме с картой, сообщает о проблеме с доставкой товара, сообщает о проблеме с доставкой товара

3 ПОПРОСИТ СДЕЛАТЬ
 Просит вас сделать переводы, сообщить о состоянии счета, сообщить о состоянии счета, сообщить о состоянии счета

4 ПРОСИТ СООБЩИТЬ ДАННЫЕ
 Просит вас сообщить данные о состоянии счета, сообщить о состоянии счета, сообщить о состоянии счета

5 НАЗЫВАЕТ ВНЕЗАПНОЕ ВЫГОДА ИЛИ СПЕЦИАЛ
 Сообщает вам о выгоде, о специи, о специи

Важно! Сотрудник банка и сотрудник НИРСИДА не сообщают данные по карте, пароли и SMS, персональные данные и не просят совершать переводы и делать звонки

НИКОГДА НИКОМУ НЕ СООБЩАЙТЕ

- свои ID (PIN)
- персональный код на авторизацию в личном кабинете (СМС-код)
- ЛИН код
- пароли/логины к банкомату/приложению и онлайн-банку
- любое слово персональные данные

Федеральная служба по техническому и экспортному контролю

Банк России

КАК ЗАЩИТИТЬСЯ ОТ ФИШИНГА

Фишинг – это мошенничество, при котором злоумышленники пытаются получить доступ к вашим персональным данным, номерам карт, паролям, PIN-кодам, номерам телефонов, адресам электронной почты, номерам счетов и другим данным.

КАК МОЖНО ОКАЗАТЬСЯ НАД ФИШИНГОВЫМ САЙТОМ?

• При посещении сайта вы видите, что адресная строка браузера не совпадает с адресом сайта, который вы хотели посетить

• Адресная строка браузера содержит адрес сайта, который вы хотели посетить, но в адресной строке вы видите, что адрес сайта не совпадает с адресом сайта, который вы хотели посетить

КАК РАСПОЗНАТЬ ФИШИНГОВЫЙ САЙТ?

• Адресная строка браузера содержит адрес сайта, который вы хотели посетить, но в адресной строке вы видите, что адрес сайта не совпадает с адресом сайта, который вы хотели посетить

• Адресная строка браузера содержит адрес сайта, который вы хотели посетить, но в адресной строке вы видите, что адрес сайта не совпадает с адресом сайта, который вы хотели посетить

КАК УВЕРИТЬСЯ ОТ ФИШИНГА?

• Убедитесь, что адресная строка браузера содержит адрес сайта, который вы хотели посетить

• Убедитесь, что адресная строка браузера содержит адрес сайта, который вы хотели посетить

• Убедитесь, что адресная строка браузера содержит адрес сайта, который вы хотели посетить

Федеральная служба по техническому и экспортному контролю

Банк России

КАК ЗАЩИТИТЬСЯ ОТ ОНЛАЙН-МОШЕННИКОВ

Чтобы избежать риска доверить свои деньги или данные, мошенникам, нужно быть всегда бдительным и внимательным к деталям.

Какие схемы используют мошенники?

• Предложение о выигрыше, о специи, о специи

• Предложение о выигрыше, о специи, о специи

• Предложение о выигрыше, о специи, о специи

Как обезопасить свои деньги и персональные данные?

1. Убедитесь, что адресная строка браузера содержит адрес сайта, который вы хотели посетить
2. Убедитесь, что адресная строка браузера содержит адрес сайта, который вы хотели посетить
3. Убедитесь, что адресная строка браузера содержит адрес сайта, который вы хотели посетить
4. Убедитесь, что адресная строка браузера содержит адрес сайта, который вы хотели посетить
5. Убедитесь, что адресная строка браузера содержит адрес сайта, который вы хотели посетить

Федеральная служба по техническому и экспортному контролю