

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



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

[https://finclass.info/\\_wt/cybergram;](https://finclass.info/_wt/cybergram;)



4. Карточки по тематике киберграмотности –

**Банк России**

## ЧТО ДЕЛАТЬ, ЕСЛИ С КАРТЫ УКРАЛИ ДЕНЬГИ?

- ЗАБЛОКИРОВАТЬ КАРТУ**  
 По телефону или лично обратившись в клиентский центр или на официальном сайте банка, скачав специальное приложение.
- НАПИСАТЬ ЗАЯВКУ НЕОСНОВАННОЙ ОПЕРАЦИИ**  
 В течение 60 дней со дня списания денег с карты вы можете обратиться в банк с заявкой на возврат денег.
- ОБРАТИТЬСЯ В ГОСУДАРСТВЕННЫЕ ОРГАНЫ**  
 Если вы обнаружили кражу денег с карты, необходимо обратиться в полицию.

**КАК ОБЕЗОПАСИТЬ ДЕНЬГИ НА СЧЕТАХ?**

**НИКОМУ НЕ СООБЩАЙТЕ:**  
 Свой номер карты и срок ее действия, код безопасности (CVV2/CVC2) и PIN-код.

**НЕ ПИШИТЕ КОДЫ:**  
 Не сообщайте никому свои персональные данные и коды безопасности.

**УСТАНОВИТЕ:**  
 Специальное приложение на свой смартфон.

**Банк не возмещает ущерб, если вы нарушили правила безопасности карты.**

Финансовая культура

**Банк России**

## ОСТОРОЖНО: ТЕЛЕФОННЫЕ МОШЕННИКИ!

### 5 ПРИЗНАКОВ ОБМАНА

- НА ВАС ВЫХОДИТ САНИ**  
 Алгоритмы и программы на сайтах мошенников часто копируют дизайн официальных сайтов. СМС или письма – повод насторожиться.
- РАДУЮТ ВНЕЗАПНОЙ ВЫГОДОЙ ИЛИ ПУЖАЮТ**  
 Сильные эмоции свидетельствуют об опасности.
- НА ВАС ДАВЯТ**  
 Авансы в виде подарков, чтобы у вас не было времени на обдумывание.
- ГОВОРЯТ О ДЕНЬГАХ**  
 Предлагают услуги, которые обещают вернуть, но не предоставляют никаких документов.
- ПРОСИТ СООБЩИТЬ ДАННЫЕ**  
 Запрашивают номер и срок действия карты, пароли и коды из банкоматов (уведомлений).

**ВАЖНО!**  
 Сотрудник банка и полиции НИКОГДА не смогут распечатать карты, пароли из СМС, персональные данные и не просят секретных паролей с вашей карты.

**НИКОГДА НИКОМУ НЕ СООБЩАЙТЕ:**  
 Коды из СМС, трехзначный код на обратной стороне карты (CVV2/CVC2), PIN-код, пароли/логины к банковскому приложению и онлайн-банку, любое слово персональные данные.

Финансовая культура

**Банк России**

## КАК ЗАЩИТИТЬСЯ ОТ ФИШИНГА

Фишинг – это мошенничество, при котором злоумышленники пытаются получить доступ к вашим данным, используя сайты, которые выглядят как официальные сайты банков.

**КАК МОЖНО ОКАЗАТЬСЯ НА ФИШИНГОВОМ САЙТЕ?**  
 При посещении официального сайта банка или почты, СМС, уведомлений и уведомлений от кредиторов, мошенники могут использовать фишинговые сайты.

**КАК РАСПОЗНАТЬ ФИШИНГОВЫЙ САЙТ?**  
 Адрес сайта не совпадает с официальным сайтом банка.  
 В адресной строке не отображены HTTPS или SSL-сертификат.  
 Дизайн сайта не совпадает с официальным сайтом банка.  
 В адресной строке не отображены HTTPS или SSL-сертификат.

**КАК УВЕРИТЬСЯ ОТ ФИШИНГА?**  
 Устанавливайте обновления на свой смартфон и компьютер.  
 Используйте надежные антивирусные программы.  
 Не сообщайте никому свои персональные данные и коды безопасности.

Финансовая культура

**Банк России**

## КАК ЗАЩИТИТЬСЯ ОТ ОНЛАЙН-МОШЕННИКОВ

Чтобы добро пасть до ваших банковских счетов, мошенникам нужны ваши персональные данные и реквизиты карт.

**Какие схемы используют аферисты?**

**ОБМАНЧИВЫЕ ВОЗВРАТНЫЕ ЧЕКИ**  
 Аферисты предлагают вернуть деньги за покупки, которые вы не делали.

**УВЕДОМЛЕНИЯ О НАСРОКОВАННОСТИ**  
 Уведомления о просрочке платежей, которые вы не делали.

**ОБЪЕДИНЕНИЕ НА ПРОВЕРКУ И СДЕЛКА**  
 Предлагается объединить счета, чтобы проверить баланс, но требуется ввести данные карты.

**НАСРОКОВАННОСТЬ**  
 Предлагается вернуть деньги за покупки, которые вы не делали.

**Как обезопасить свои деньги в интернете?**

- Делайте резервные копии своих данных.
- Держите в тайне любые данные, которые вы вводите в интернет.
- Используйте надежные антивирусные программы.
- Не сообщайте никому свои персональные данные и коды безопасности.
- Используйте надежные пароли и коды безопасности.

Финансовая культура