Приложение 1

# Как не поддаться на уловки кибермошенников

Кибермошенничество - один из видов преступлений в Интернете, целью которого является причинение материального или иного ущерба путем хищения личной информации пользователя (номера банковских счетов, паспортные данные, коды, пароли и др.).

Злоумышленники для достижения целей воздействуют на эмоции, страхи и рефлексы людей и побуждают перейти по вредоносной ссылке.
При переходе по ссылке человек попадает на фишинговый сайт, где его просят ввести персональные или банковские данные.
Очень часто в сообщениях содержатся ссылки на вредоносное ПО.



ПРАВИТЕЛЬСТВО ЛЕНИНГРАДСКОЙ ОБЛАСТИ

## Наиболее распространенные схемы онлайн-мошенничества

### ВАША УЧЕТНАЯ ЗАПИСЬ БЫЛА ИЛИ БУДЕТ ЗАБЛОКИРОВАНА / ОТКЛЮЧЕНА

Перед угрозой блокировки аккаунта пользователь теряет бдительность, переходит по ссылке в письме и вводит свои логин и пароль.

### В ВАШЕЙ УЧЕТНОЙ ЗАПИСИ ОБНАРУЖЕНЫ ПОДОЗРИТЕЛЬНЫЕ ИЛИ МОШЕННИЧЕСКИЕ ДЕЙСТВИЯ. ТРЕБУЕТСЯ ОБНОВЛЕНИЕ НАСТРОЕК БЕЗОПАСНОСТИ

В таком письме пользователя просят срочно войти в учетную запись и обновить настройки безопасности. Пользователь паникует и забывает о бдительности.



ПРАВИТЕЛЬСТВО ЛЕНИНГРАДСКОЙ ОБЛАСТИ

## Наиболее распространенные схемы онлайн-мошенничества:

### ВАШ ДРУГ ОСТАВИЛ ВАМ СООБЩЕНИЕ. ПЕРЕЙДИТЕ ПО ССЫЛКЕ, ЧТОБЫ ПРОЧИТАТЬ

В подобных письмах злоумышленники скрываются за маской людей/организаций, которые входят в ваш доверенный круг, чьи письма и сообщения не должны у вас вызвать подозрений. Люди склонны идти навстречу тем, кому доверяют: переходят по ссылке в письме и вводят свои личные данные.

### ПИСЬМА ОТ ГОСУДАРСТВЕННЫХ СЛУЖБ

Фишинговые письма приходят от имени различных госорганов с информацией о претензиях, которые возникли к пользователю со стороны государства. Чаще всего в письмах фигурируют МВД, ФНС и ФМС, а также организации системы здравоохранения.



ПРАВИТЕЛЬСТВО ЛЕНИНГРАДСКОЙ ОБЛАСТИ

## Наиболее распространенные схемы онлайн-мошенничества

### СОЦИАЛЬНАЯ ПОДДЕРЖКА

Благотворительность и меценатство — любимые темы злоумышленников. Чем эмоциональнее обращение к вам, тем больше оснований подозревать мошенничество.
Популярные темы писем: благотворительность после стихийных бедствий, человек в беде, сборы на лечение.

### ВЫ ВЫИГРАЛИ

Сообщение о выигрыше и ссылкой на сайт, где якобы можно получить приз.



ПРАВИТЕЛЬСТВО ЛЕНИНГРАДСКОЙ ОБЛАСТИ

## Лучшая защита от кибермошенников – соблюдение правил цифровой гигиены:

- Используйте только лицензионное ПО, регулярно его обновляйте и включайте антивирусную защиту на всех устройствах.

- Важные файлы храните не только на жестком диске компьютера, но и на внешних жестких дисках или в облачном хранилище.

- Используйте двухфакторную аутентификацию, например, для защиты электронной почты. Обязательны сложные пароли из незначащих комбинаций букв, цифр и знаков, не менее 8 символов. Не используйте один и тот же пароль для разных систем. Меняйте пароли хотя бы раз в полгода.

ПРАВИТЕЛЬСТВО ЛЕНИНГРАДСКОЙ ОБЛАСТИ

## Лучшая защита от кибермошенников – соблюдение правил цифровой гигиены:

- Проверяйте вложения, полученные по электронной почте, с помощью антивирусного ПО. С осторожностью относитесь к сайтам с некорректными сертификатами. Будьте внимательны при вводе учетных данных на сайтах и во время работы с онлайн-платежами.

- Не переходите по ссылкам на незнакомые ресурсы, особенно если браузер предупреждает о рисках. Игнорируйте ссылки из всплывающих окон, даже если компания или продукт вам знакомы. Не загружайте файлы с подозрительных веб-ресурсов.

- Заведите отдельную карту для оплаты товаров в Интернете и подключите оповещения по операциям на счете карты.

ПРАВИТЕЛЬСТВО ЛЕНИНГРАДСКОЙ ОБЛАСТИ