

# Не попадитесь на удочку мошенников



## Основные темы фишинговых писем

### Онлайн-сервисы

Подписки на онлайн-кинотеатры, музыку, книги

### Туроператоры

Путёвки и бронирование отелей и билетов

### Службы доставки

Статус доставки товара, акции с подарками за доставку

### Госуслуги

Бонусы за участие в опросах, социальные выплаты, поддержка по актуальным вопросам

## Опасные темы-крючки – 2023



### Мобилизация

«Проверьте список»; «Получите отсрочку»; «Поможем избежать мобилизации».



### Цифровая валюта

«О, счастливец! Ты выиграл биткоины. Скорее перейди по ссылке и оставь данные своего кошелька».



### Заработок в интернете

Предложения «стабильного дохода» от известных брендов.



### Штраф из налоговой

«За вами числится задолженность, срочно оплатите».



### Недоступные видео теперь доступны

Кинопремьеры эксклюзивно и по выгодным ценам

**Если сайт вызывает малейшие подозрения, не пользуйтесь им!**

## Где скрывается обман?

 <b>Просьба ввести пароль или логин</b> <i>Письмо от банка с предупреждением о взломе аккаунта. Чтобы поменять логин и пароль, нужно срочно перейти по ссылке в письме и ввести старые логин и пароль</i> Помните, что ни один реальный банк (сервис, доставка, служба и пр.) не станет спрашивать ваши пароль и логин	 <b>Ошибки в словах</b> <i>«отправьтепароль» или «отправте пароль»</i> Чтобы обойти спам-фильтры, установленные на слова-триггеры, мошенники изменяют слова и пишут их с ошибками	 <b>Предложение перейти по ссылке</b> <i>имясайта.чтоугодно.com</i> Наведите курсор на ссылку (не нажимая), внизу слева появится реальный адрес, на который она ведёт. Правильный адрес может выглядеть примерно так: <a href="https://www.sberbank.ru">https://www.sberbank.ru</a>	
 <b>Неизвестный доменный адрес</b> <i>юрийпетрович@кмпния1.ру</i> Мошенники незначительно меняют имя домена, рассчитывая на вашу невнимательность. Такой Юрий Петрович вам не нужен!	 <b>Изменённые названия известных брендов</b> <i>aplle.com или qoogle.com</i> Дело «Abibas» живет! Расчёт на вашу невнимательность и незнание точного названия брендов	 <b>Срочность</b> <i>«срочная проверка»; «блокировка через 60 минут»</i> Мошенникам важно, чтобы вы не успели задуматься!	 <b>Обезличенное обращение</b> <i>Уважаемый сотрудник!</i> «Ковровая бомбардировка» по всем, кто хочет быть обманутым

Если вы ввели данные своей банковской карты на фишинговом сайте — звоните по номеру 900

## Что изучить ещё



Узнайте больше о безопасности в интернете



Больше информации — в библиотеке знаний по кибербезопасности «Кибрарий»