УВД ГОМЕЛЬСКОГО ОБЛИСПОЛКОМА

КРИМИНАЛЬНАЯ МИЛИЦИЯ

УПРАВЛЕНИЕ ПО ПРОТИВОДЕЙСТВИЮ КИБЕРПРЕСТУПНОСТИ

ОПОРНЫЙ ПЛАН-КОНСПЕКТ

Тема:

«Что такое фишинг? Как защитить себя от фишинга»

Гомель

2022 год

За последние десятилетия число киберпреступлений в мире увеличилось в огромное количество раз, мотивы и цели киберпреступников менялись с течением времени, а опасность совершаемых преступлений возрастает с каждым годом. Этому свидетельствуют огромные финансовые потери юридических лиц
и структур, а также участившиеся случаи киберпреступлений и против физических лиц.

В Гомельской области с 2017 года наблюдался устойчивый рост таких преступлений (2017 г. – 370, 2018 г. – 563, 2019 г. – 1781, 2020 г. – 3394). В 2022 году количество преступлений снизилось, за 2 месяцев текущего года в Гомельской области зарегистрировано 295 киберпреступлений, что в 1,9 раза меньше данного показателя 2021 года (561 преступление). Более 90% из выявленных преступлений составляют хищения имущества путем модификации компьютерной информации
(ст. 212 УК Республики Беларусь). Кроме этого, отмечается рост количества преступлений в сфере информационной безопасности (28).

В дальнейшем прогнозируется, что развитие IT-отрасли
и финансово-кредитной сферы, будут способствовать сохранению тенденции совершения преступлений по направлению противодействия киберпреступности.

В национальном сегменте сети Интернет Республики Беларусь наблюдается значительное повышение мошеннической активности, связанной с использованием **фишинговых страниц** и даже целых сайтов.

Целью данной разновидности фишинга является получение
не только учетных данных от каких-либо сервисов (логин и пароль),
но и данных платежной карты (номер, срок действия, имя и фамилия держателя и CVC2/CVV2 код).

Также стоит отметить, что продуманный целевой фишинг
не обходится без использования социальной инженерии. Причем если раньше в основном происходила рассылка фишинговых писем
на электронную почту, где была возможность блокировать массовые рассылки, то теперь злоумышленники используют еще мессенджеры
и социальные сети, что значительно расширяет целевую аудиторию.

**Фишинг** — это распространенный способ интернет-мошенничества. Хакеры используют его, чтобы получить доступ к конфиденциальной информации других людей: их учетным записям и данным банковских карт.

Фишинговые мошенники действуют по отработанной схеме: закидывают «наживку» — письмо, сообщение, ссылку на сайт — и пытаются «поймать» доверчивых пользователей. Поэтому неудивительно, что сам термин произошел от англоязычного phishing, которое созвучно со словом fishing — «рыбалка». Замена f на ph — отсылка к оригинальной форме хакерства фрикингу, или телефонному взлому (phreaking).

Фишинг становится популярнее с каждым годом. Только в 2022 году в Гомельской области совершено киберпреступлений данным способом 57%.

## Виды фишинговых атак

### **Почтовый фишинг**

Злоумышленники отправляют пользователям письма под видом известного бренда: подделывают адрес, чтобы он напоминал официальный. Получатель нажимает на ссылку и переходит на поддельный сайт или загружает документ с вирусом.

Одна из вариаций почтового фишинга — **клон-фишинг**. Мошенники определяют, какими программами и магазинами вы часто пользуетесь, а затем отправляют письма якобы от этих брендов.



Пример фишингового письма, замаскированного под письмо от службы безопасности Gmail. При наведении на кнопку «Сменить пароль» отображается фишинговая ссылка.

### **Телефонный фишинг**

Этот тип атаки разделяется на два подвида: вишинг и смишинг.

**Голосовой фишинг**, или вишинг (vishing) предполагает разговор по телефону. Преступник звонит жертве, давит на нее и создает повышенное чувство срочности, чтобы человек сообщил конфиденциальные данные.

Мошенники часто представляются сотрудниками банков: они сообщают о заявках на кредит или подозрительных переводах, угрожают блокировкой, а затем требуют сообщить смс-код или оформить подозрительный перевод.

В результате люди теряют все свои накопления. Так, в 2022 году с помощью голосового фишинга мошенники [украли](https://www.rbc.ru/finances/18/05/2021/60a41a189a7947f480c3f726) у одних пенсионеров из г. Мозыря 120 тысяч белорусских рублей.

В **смишинге** (smishing) вместо звонков используют СМС-сообщения с вредоносными ссылками, которые маскируют под купоны и розыгрыши.



Пример фишингового сообщения: справа переписка с настоящим банком, слева — с мошенниками, которые переставили буквы в названии банка местами.

### **Фишинг в социальных сетях**

Такие мошенники создают поддельные аккаунты в Instagram\*, ВКонтакте, Facebook\*, Twitter. Хакеры выдают себя за знакомого жертвы или аккаунт известной компании. Они присылают сообщения со ссылками на поддельные сайты, запрашивают личную информацию через Facebook\*-приложения, отмечают на изображениях с призывом перейти на сайт.

Смежный способ фишинга — мошенничество в мессенджерах: Telegram, WhatsApp и Viber. Через них хакеры рассылают сообщения якобы от популярных компаний в попытке завладеть вашими личными данными.

Примером таких мошеннических действий служит создание поддельных аккаунтов от имени известных компаний, которые призывают ответить на некоторые вопросы и затем получить приз. Обязательно для получения приза необходимо заполнить свои личные данные и реквизиты банковской карты. Завладев такой в дальнейшем злоумышленники ее используют в преступных целях.

### **Веб-фишинг**

Главный метод этого вида — **подмена сайта**. Хакер создает страницу, практически не отличимую от сайта крупного бренда или компании, в которой вы работаете. Вы используете свою учетную запись для входа, и злоумышленник получает доступ к реальному аккаунту.



Пример фишингового сайта, замаскированного под страницу обновления Google Chrome. Адрес страницы не имеет никакого отношения к браузеру.

У веб-фишинга много вариаций.

* **Фишинг через поисковые системы**. Такие мошенники выбирают людей, желающих что-то купить: их просят ввести конфиденциальную информацию, которую перехватывает хакер.
* **Всплывающие окна** или уведомления веб-браузера. Когда человек кликает на кнопку «разрешить», на устройство загружается вредоносный код.

## Как распознать фишинг-атаки и не попасться на удочку

**Обучайтесь сами и обучайте сотрудников.**Вот список подозрительных «флажков», которые указывают на фишинговое письмо:

* Письмо создает иллюзию срочности и вызывает тревогу.
* Письмо обезличено, к отправителю не обращаются по имени (этот пункт может не соблюдаться при использовании целевого фишинга).
* В письме есть грамматические и орфографические ошибки.
* Письмо пришло от подразделения или от сотрудника, который прежде с вами не общался, либо в письме содержится нехарактерная просьба.
* К письму прикреплен zip-файл или большое изображение.
* Адрес почты вызывает подозрения. Например, организация использует адреса в виде name@example.com, а письмо пришло с адреса name.example@gmail.com. Либо в имени сотрудника есть опечатки.
* Ссылки встроены в текст или сокращены, либо при наведении на ссылку отображается другой адрес.
* Отправитель пишет с личной электронной почты вместо рабочей.

А вот как определить фишинговый сайт:

* Веб-адрес написан с ошибками: например: appel.com вместо apple.com.
* В адресе сайта стоит http вместо https.
* У адреса неправильный домен верхнего уровня: например, .org вместо .by.
* Логотип компании плохого качества.
* Браузер предупреждает, что сайт небезопасный.

**Подключите двухфакторную аутентификацию.** Двухфакторная аутентификация, помимо пароля, обычно требует:

* ввести код, который пришел на почту, в смс или в push-уведомлении;
* подтвердить вход на другом устройстве;
* подтвердить вход через биометрические данные — отпечаток пальца или сканирование лица.

Так как злоумышленники чаще всего охотятся за логинами и паролями, такая защита личных и рабочих аккаунтов пресечет многие попытки украсть данные.

**Регулярно обновляйте софт.**Злоумышленники часто используют уязвимости программного обеспечения. Чтобы избежать проблем, регулярно устанавливайте обновления, которые устраняют эти недостатки.

**Установите надежный антивирус.**Антивирусные программы сегодня не только сканируют загружаемые программы на предмет вредоносных кодов, но и могут определять фишинговые сайты.



Nod32 предупреждает, что вы пытаетесь зайти на фишинговый сайт

**Подключите почтовые фильтры**. Фишинговые мошенники часто делают массовые рассылки, поэтому хороший почтовый фильтр пометит их как [спам-рассылку](https://www.unisender.com/ru/blog/idei/spam-rassylka/).

Кроме того, киберпреступники часто прячут вредоносный код в активном содержимом PDF-файла или в коде — вы можете настроить почтовый клиент или антивирус так, чтобы сервис проверял такие вложения.

У разных почтовых клиентов фильтры настраиваются по-разному. Например, в почте Gmail можно помечать подозрительные письма ярлыками или сразу удалять их, а в Microsoft Exchange Online — основательно проверять вложения.

Чаще всего отрегулировать почтовые фильтры можно в настройках почтовых клиентов в разделах «Фильтры» или «Правила».



Пример фильтров, которые можно настроить в Gmail



Пример настройки правил для вложений в Microsoft Exchange Online

## Главные мысли

