В условиях повсеместной цифровизации общества и использования информационных систем как в повседневной жизни, так и рабочей деятельности важную роль играет киберграмотность пользователей.

Наиболее популярными и эффективными способами проникновения в инфраструктуру компании являются эксплуатация уязвимостей системы защиты информации и использование социальной инженерии для атаки на сотрудников.

Основы кибергигиены и понимание, что это такое, какими методами пользуются киберпреступники и как от них защититься, позволят сделать вашу жизнь и работу более безопасной.

В данной рассылке основное внимание уделено *наиболее распространённому* виду социотехнических кибератак – **фишингу**.

Общие рекомендации по кибергигиене находятся в разделе «Рекомендации»

1. Фишинг

Фишинг – это вид атак социальной инженерии, цель которого – получение конфиденциальных данных пользователя. Этими данными могут быть как пароль и логин, так и данные банковской карты или персональные данные.

Фишинг основывается на незнании человеком основ безопасности в сети: **любые сервисы/компании/банки НЕ РАССЫЛАЮТ письма с просьбами указать свои учётные данные, пароли, логины и т.д.**

1.1. Типы фишинга

1.1.1. Адресный фишинг и уэйлинг

Как и в обычных фишинговых атаках, в **адресном (целевом) фишинге** и уэйлинге ***для обмана*** жертв ***используются электронные письма из надежных источников***. Однако вместо массовой рассылки множеству получателей ***адресный фишинг нацелен на конкретных лиц*** или ***выдает себя за вызывающее доверие лицо*** для кражи учетных данных или информации.

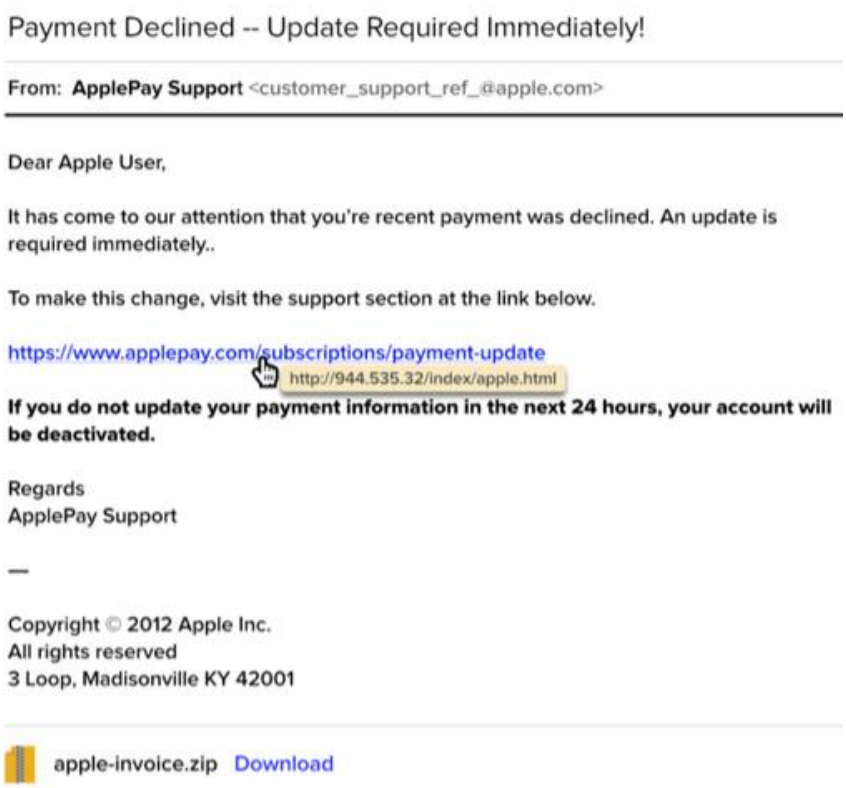
Уэйлинг (с англ. whaling — «охота на китов») ***направлен на*** конкретное ***высокопоставленное лицо***. Вместо того, чтобы нацеливаться на широкую группу, такую как отдел или команда, злоумышленники направляют своего внутреннего капитана Ахава на высокоуровневые цели — руководителей и влиятельных лиц — в надежде поразить своего белого кита.

1.1.2. Клон-фишинг

Этот метод атаки заключается в ***полном копировании письма*** **легитимной организации** (например, 21vek.by, Belarusbank) и ***подменяют*** **ссылки**, которые перенаправляют пользователя на мошеннический сайт.

1.2. Небольшое тестирование

Давайте представим ситуацию, что Вы получили такое письмо на свою электронную почту. Как Вы считаете, оно действительно пришло от ApplePay?


Payment Declined -- Update Required Immediately!

From: **ApplePay Support** <customer_support_ref_@apple.com>

Dear Apple User,

It has come to our attention that you're recent payment was declined. An update is required immediately..

To make this change, visit the support section at the link below.

https://www.applepay.com/subscriptions/payment-update

http://944.535.32/index/apple.html

If you do not update your payment information in the next 24 hours, your account will be deactivated.

Regards
ApplePay Support

—

Copyright © 2012 Apple Inc.
All rights reserved
3 Loop, Madisonville KY 42001

apple-invoice.zip Download

Рисунок 1 – Входящее письмо

Допустим, Вы решили перейти по ссылке и видите следующий сайт. На Ваш взгляд, он действительно является веб-сайтом ApplePay

Рисунок 2 – Сайт ApplePay

Как Вы могли понять, и сайт, и письмо являются мошенническими. Обратите внимание! На рисунке те части письма и веб-сайта, на которые являются сигналом, что ресурс нелегитимный.

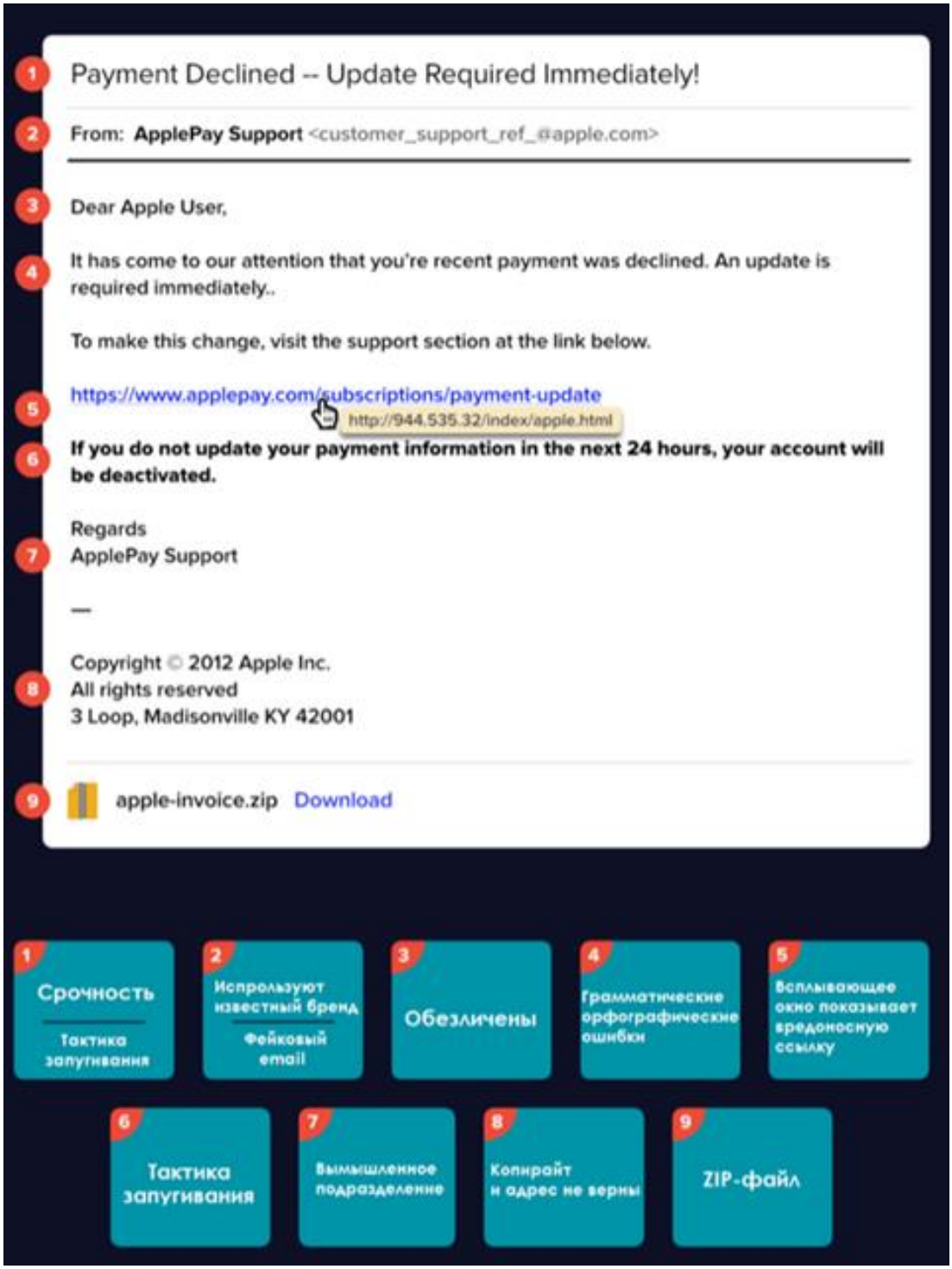


Рисунок 2 – Фишинговое письмо

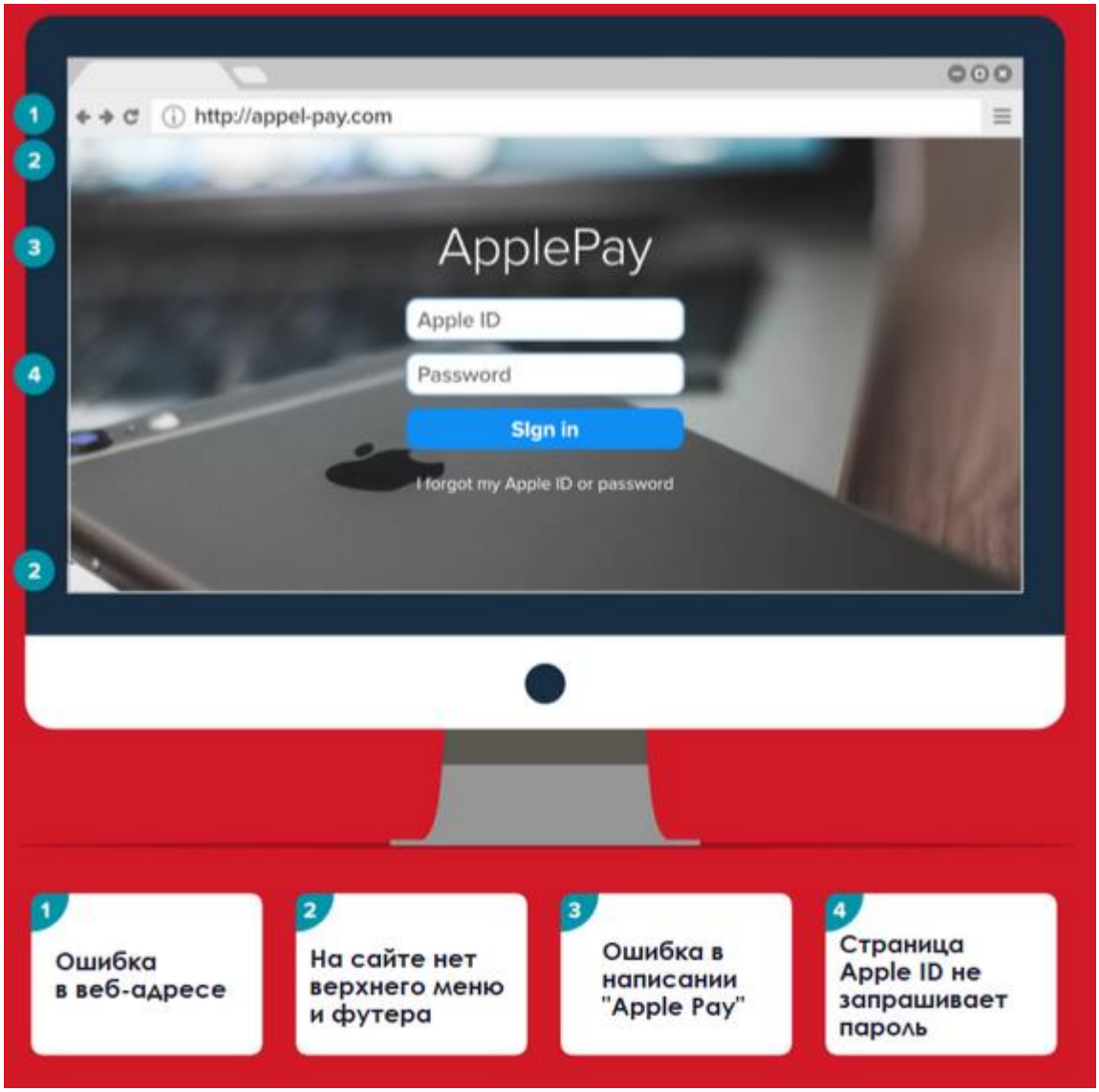


Рисунок 4 – Фишинговый веб-сайт

1.3. Как себя защитить?

Какими бы ни были изобретательными ***фишинговые письма***, они **всегда имеют *схожую анатомию***.

Чему же стоит уделить внимание?

1.3.1. Со стороны отправителя

− Письмо получено ***от человека***, которого Вы **не знаете** либо **контактируете очень редко**;

− Вы **не доверяете**, **не поддерживаете** деловые отношения с ним или **никогда прежде не контактировали** с отправителем;

− Вы **знаете отправителя**, но **стиль письма очень подозрителен**;

− ***Почтовый адрес отправителя*** отображается с явной **грамматической ошибкой**.

1.3.2. Со стороны получателя

− Письмо **адресовано** ***не только вам***, но и другим людям, с которыми вы не знакомы.

1.3.3. Ссылки

− В письме **указан** ***один адрес***, **но** **при переходе** по нему, браузер **перенаправляет** Вас ***по совершенно другому*** адресу;

− Письмо содержит **исключительно ссылку**;

− Ссылка содержит **адрес**, который **похож** ***на популярный сайт***, но имеет явные **грамматические ошибки**.

1.3.4. Время получения

− Например, получатель письма – менеджер компании, который вдруг видит входящее письмо от другого работника фирмы, но отправленное очень глубокой ночью.

1.3.5. Суть письма

− ***Тема*** письма **не соотносится** с его **содержанием**;

− **Тема** отображается **как будто ответ** на письмо, которое Вы **никогда** в действительности **не видели** **и не** **отправляли**.

1.3.6. Содержание письма

− В письме содержится **срочный призыв к действию** – перейти по предоставленным ссылкам, чтобы избежать чего-то глобального и негативного;

− В тексте **много ошибок** и его **стиль написания** вызывает вопросы;

− Отправитель ***настоятельно*** **просит отправить** **ваши персональные данные** или подтвердить нужную ему верификацию по СМС-сообщению.

2. Рекомендации

Таблица 1 – Общие рекомендации по кибергигиене

Необходимо:	**Не рекомендуется:**
Защита данных банковской платежной карточки	
Хранить в тайне пин-код, сведения с карточки сеансовых кодов	Хранить пин-код вместе с карточкой/на карточке
Прикрывать ладонью клавиатуру при вводе пин-кода	Сообщать кому-либо реквизиты карты или отправлять их фото по сети Интернет
Оформить отдельную карту для онлайн-покупок, выезда за границу, и не хранить на ней большие суммы. Для карты, используемой в Беларуси, рекомендуется ограничить возможность ее использования за пределами нашей страны	Распространять свои персональные данные (информацию личного характера, номер мобильного телефона), логин и пароль доступа к системе «Интернет-банкинг»
Использовать двухфакторную аутентификацию, установить лимиты на максимальные суммы операций, подключить смс-оповещение о проведении операций по карте	Сообщать данные, полученные в виде SMS-сообщений: сеансовые пароли, код авторизации, пароль «3-D Sequre» и т.д.
Скрыть CVV номер на карте (трехзначный номер на оборотной стороне), предварительно сохранив его	Пользоваться системой «Интернет-банкинг» на чужих компьютерах или мобильных устройствах
Вводить логин и пароль к системе «Интернет-банкинг» только на официальном сайте или в мобильном приложении банка	
В случае утери (кражи) карты, незамедлительно по телефону обратиться в банк для ее блокирования	
При обнаружении несанкционированного списания денежных средств с карт-счета, незамедлительно обратиться с заявлением в банк для их возврата по принципу «нулевой ответственности»	

Безопасность электронной почты	
Подключить двухфакторную аутентификацию	Реагировать на письма от неизвестного отправителя: скорее всего, это спам или «фишинговая» рассылка
Использовать минимум 2 типа e-mail адресов: закрытые (только для привязки устройств и средств защиты, интернет-банкинга и др.), открытые (отдельные для переписки, регистрации на форумах, оформления различных подписок и т.д.)	Открывать подозрительные вложения к письму: сначала позвоните отправителю и узнайте, что это за файл
Использовать спам-фильтры и соответствующее антивирусное программное обеспечение	Отправлять в открытом виде важные данные (фотоизображения документов, пароли и т.д.). В случае необходимости – заархивировать, установив сложный пароль
В случае подозрительных ситуаций проверить статистику подключений и изменить пароль	
Использование браузеров и сайтов	
Использовать специальное программное обеспечение (антивирус, расширение для браузера), чтобы избежать неблагоприятных последствий после посещения зараженных сайтов	Переходить по непроверенным ссылкам и посещать сайты сомнительного содержания
Производить регулярное обновление ПО, антивирусов и файерволов	Вводить информацию на сайтах, если соединение не защищено (нет https)
Обращать внимание при авторизации на доменное имя интернет-ресурса (может произойти подмена имени сайта с целью «фишинга»)	Открывать всплывающие окна, рекламные баннеры и устанавливать предлагаемое неизвестными сайтами ПО

Использование приложений, соцсетей и мессенджеров	
По возможности скрывать номер телефона, адрес электронной почты и другие сведения	Размещать персональную и контактную информацию о себе в открытом доступе
Обмениваться сообщениями в соцсетях и мессенджерах только полностью удостоверившись в личности собеседника, не реагируя на сомнительные просьбы и предложения	Использовать указание геолокации на фото и постах
Устанавливать программное обеспечение только из достоверных источников	Отвечать на обидные выражения и агрессию в соцсетях – лучше написать об этом администратору ресурса
Безопасность мобильных устройств	
Использовать пин-код, а также дополнительные способы блокирования устройства (графический ключ, пароль, отпечаток пальца и др.)	Передавать незнакомым мобильный телефон или сим-карту. В случае передачи – контролировать все действия, которые производятся с устройством
Своевременно обновлять операционную систему устройства, антивирус и др. ПО	Устанавливать приложения с низким рейтингом и отрицательными отзывами
Устанавливать приложения из PlayMarket, AppStore или только из проверенных источников	Перезванивать на незнакомые иностранные номера
Обращать внимание, к каким функциям гаджета приложение запрашивает доступ	Хранить важную информацию на мобильном устройстве
Включить встроенные функции устройства для определения его местонахождения	Делать полное снятие ограничения на устройстве («джейлбрейк», режим «суперюзера»)
В случае утери (кражи) устройства, незамедлительно сменить пароли к интернет-банкингу, электронной почте и другим сервисам, а также обратиться в правоохранительные органы	

Безопасность мобильных устройств	
При смене абонентского номера обязательно изменить привязку интернет-сервисов к новому номеру (лучше сделать это заблаговременно)	
При продаже устройства произвести его сброс до заводских настроек	
Безопасный Wi-Fi	
После установки устройства для доступа к Wi-Fi сразу же поменять пароль и логин, установленные по умолчанию	Вводить свой логин и пароль доступа к учетной записи (странице) или системе банковского обслуживания при подключении к бесплатным (открытым) точкам Wi-Fi в кафе, транспорте, торговом центре и т.д.
Использовать надежный пароль для доступа к вашей Wi-Fi точке	Включать общий доступ к своей Wi-Fi точке, даже если у вас безлимитный Интернет
Деактивировать автоматическое подключение своих устройств к открытым Wi-Fi точкам	