Министерство образования Республики Беларусь

Учреждение образования
«Белорусский государственный университет информатики и радиоэлектроники»

Кафедра защиты информации

ОПРЕДЕЛЕНИЕ ПРИЗНАКОВ ФИШИНГА ПО СОДЕРЖАНИЮ СООБЩЕНИЙ ЭЛЕКТРОННОЙ ПОЧТЫ

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

к практическим занятиям по дисциплине
«Методология информационной безопасности»

для студентов специальности
1-98 01 02 «Защита информации в телекоммуникациях»

Минск 2021

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 6
«ОПРЕДЕЛЕНИЕ ПРИЗНАКОВ ФИШИНГА ПО СОДЕРЖАНИЮ СООБЩЕНИЙ ЭЛЕКТРОННОЙ ПОЧТЫ»

Цель занятия: изучить признаки фишинга содержащихся в сообщениях электронной почты и получить практические навыки их обнаружения в таких сообщениях.

1 Краткие теоретические сведения

Во многих организациях мира в основе обеспечения бизнес-процессов лежит применение электронной почты, которая позволяет передавать не только текстовые сообщения, но и различные файлы. Проверка подлинности сообщения переданного по электронной почте на широко используемых почтовых ресурсах в корпоративных и глобальных информационных сетях затруднительна. Для обеспечения безопасности информации, которая принимается, передается, обрабатывается и хранится в информационных системах, используются средства защиты информации, которые ограничивают к ней доступ посредством парольной защиты. Такое положение дел в информационных системах обуславливает проблему фишинга.

Фишинг (phishing – выуживание идентификаторов) – способ получения идентификаторов пользователя информационных систем (логин, пароль, данные платежной карты и т.д.) нарушителем, который основан на предоставлении пользователю такой информации и создании нарушителем таких условий ее восприятия, при которых пользователь примет ошибочное решение и в результате чего выполнит некоторое действие, которое является выгодным для нарушителя (передача идентификаторов, загрузка вредоносной программы).

Фишинг ориентирован на введение в заблуждение пользователя информационной системы, но его критическое мышление является барьером при принятии им ошибочного решения. Поэтому понимая, что в уравновешенном эмоциональном состоянии пользователь не может совершить необходимые для нарушителя действия, нарушитель обязан изменить его эмоциональное состояние таким образом, чтобы нейтрализовать его критическое мышление на то время, когда он будет совершать выгодное действие для нарушителя. В этом заключается сущность ***социальной инженерии***, как методе управления действиями пользователя информационной системы.

Критическое мышление – способность человека, заключающаяся в проведении анализа получаемой им информации, за счет сопоставления анализируемых им сведений и накопленной ранее достоверной информации с целью выявления их не соответствия с последующим отвержением не соответствующих сведений.

Фишинг делится на два вида:

1. ***Почтовый*** – сообщения, которые формирует нарушитель, передаются посредством электронной почты. Такие сообщения кроме текста содержат, вложения в виде файла (рисунок 1) или гипертекстовой ссылки на файл (рисунок 2), загрузка которого или переход по которой приводит к загрузке и установке вредоносной программы на устройство пользователя (например, персональный компьютер, смартфон и т.д.). Этот вид фишинга приводит к несанкционированному доступу нарушителя к информационной системе, в результате которого могут произойти следующие события:

- выгрузка данных с устройства пользователя и при определенных условиях из информационной системы, куда его устройство подключено, для дальнейшей их продажи;

- получение всех идентификаторов пользователя к его учетным записям, которые он использует на данном устройстве;

- запуск вредоносной программы – шифровальщика, для получения выкупа за расшифрование информации на данном устройстве.

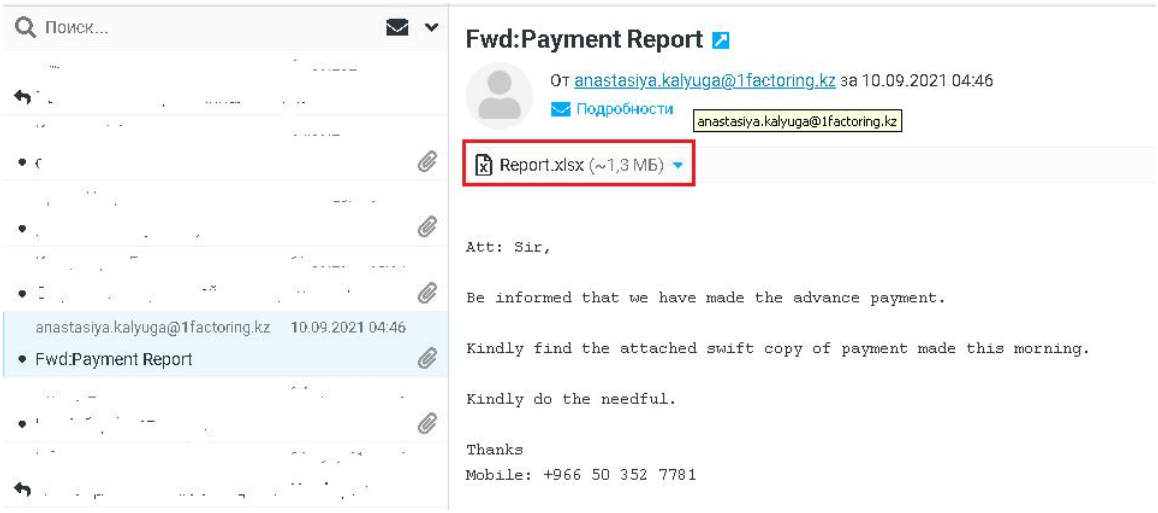

Рисунок 1. – Фишинговое почтовое сообщение с вложенным файлом

2. ***Онлайновый*** – сообщения, которые формирует нарушитель, передаются посредством электронной почты и содержат кроме текста

гипертекстовую ссылку или ссылку в виде «кнопки» (рисунок 3) переход по которым приводит к загрузке сайта, контролируемого нарушителем, где пользователю будет предложено ввести свои идентификаторы (рисунок 4).

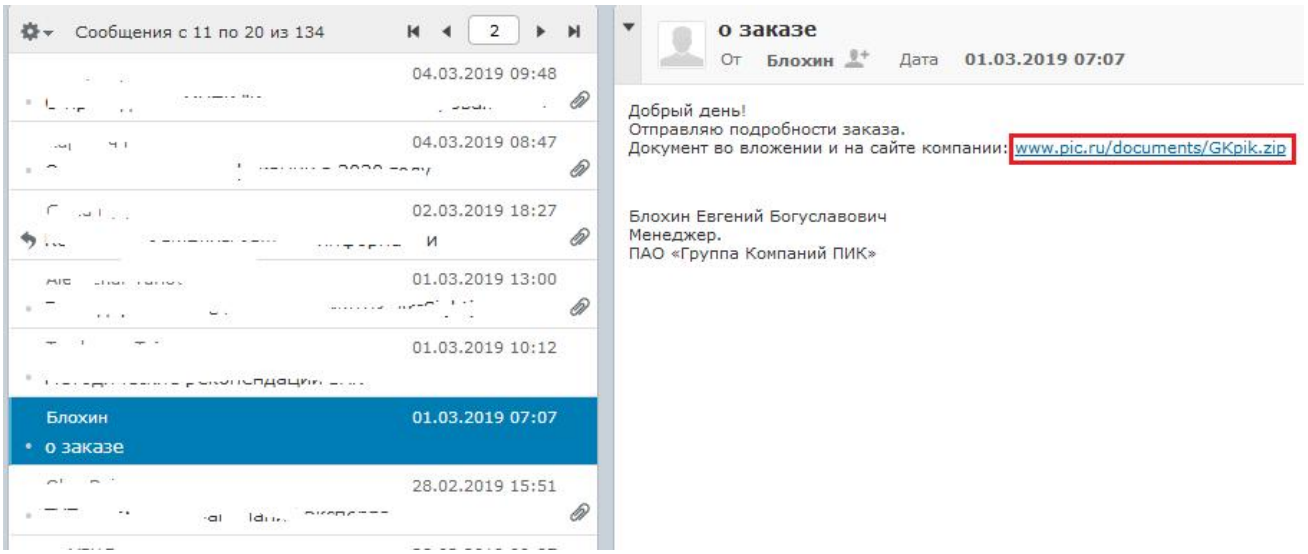

Рисунок 2. – Фишинговое почтовое сообщение с гипертекстовой ссылкой на файл

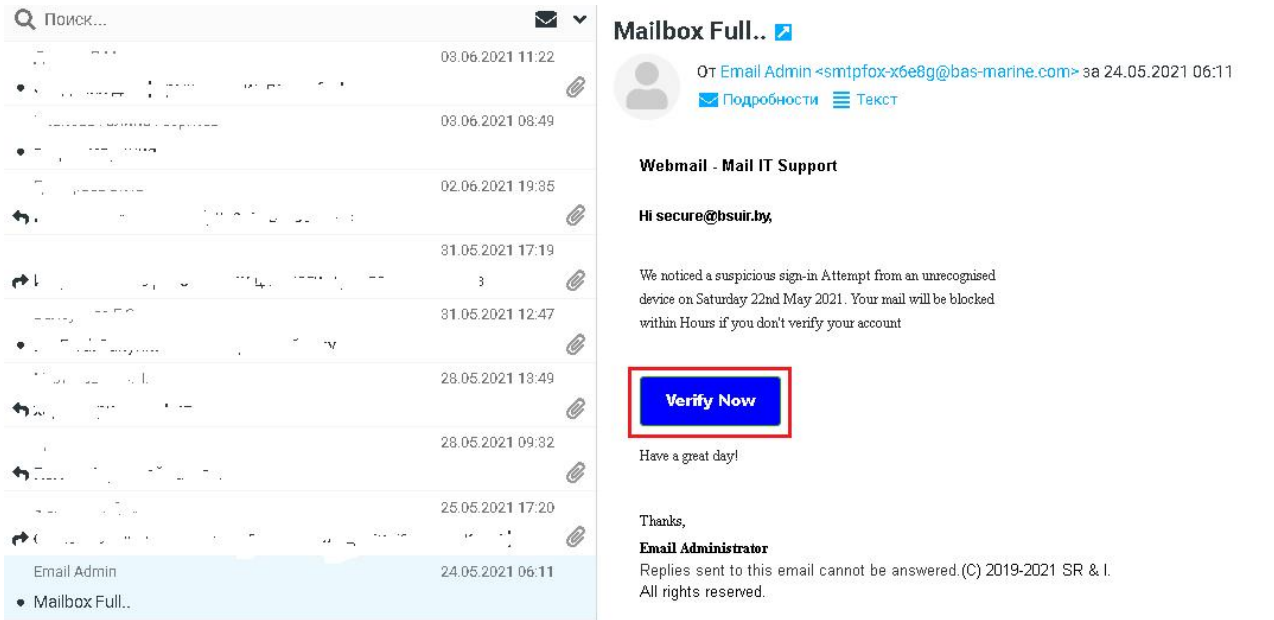

Рисунок 3. – Фишинговое почтовое сообщение со ссылкой в виде «кнопки»

3. ***Целенаправленный (спиарфишинг, spear - гарпун)*** - сообщения, которые формирует нарушитель, передаются посредством электронной почты. Их текст адресован конкретному человеку, так как нарушитель до составления

такого сообщения смог получить доступ к персональным данным этого человека (рисунок 5).

4. ***Вишинг*** – вид фишинга реализуемый с помощью средств IP (IP –internet protocol) телефонии (мессенджеры). В этом случае пользователь мессенджера получает входящий голосовой вызов на свой смартфон от нарушителя (рисунок 6). Управление действиями пользователя по передаче им идентификаторов нарушителю обеспечивается в процессе беседы с ним нарушителя. Этот вид фишинга ориентирован на получение денежных средств, поэтому нарушитель будет просить сообщить ему либо данные платежной карты, либо перевести деньги на его счет. Отличие вишинга от других видов фишинга заключается в том, что нарушитель будет стараться не дать время человеку на размышление о целесообразности того или иного действия. При почтовом же фишинге у пользователя электронной почты времени на обдуманное принятие решения больше.

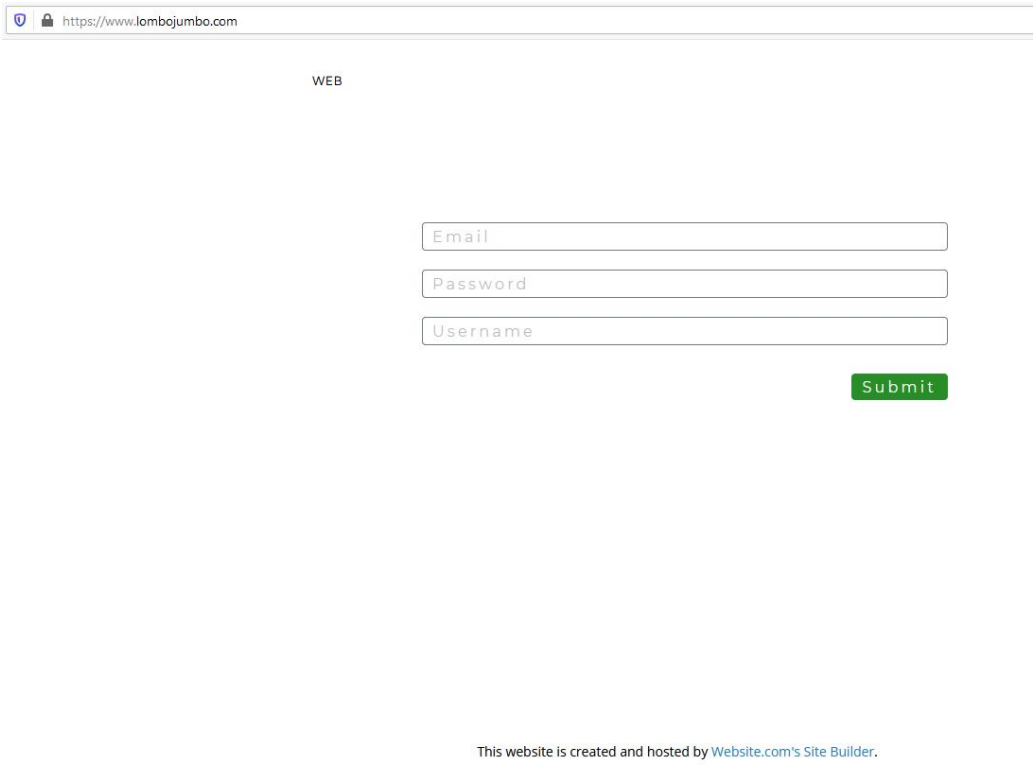

Рисунок 4. – Внешний вид фишингового сайта для сбора идентификаторов электронной почты

Для изменения эмоционального состояния пользователя информационной системы нарушитель может использовать одну из следующих тактик:

1. Сообщить ему о некоторой существенной для него проблеме, и пока эмоциональное состояние человека не пришло в норму – предложить ему

помощь в решении обозначенной нарушителем проблемы (тактика «страха»). Суть помощи будет сводиться к завладению нарушителем идентификаторами пользователя. В данном случае на эмоциональное состояние человека воздействует страх. Пока он испуган – им можно управлять. Это классика фишинга, так бесстрашных людей не бывает.

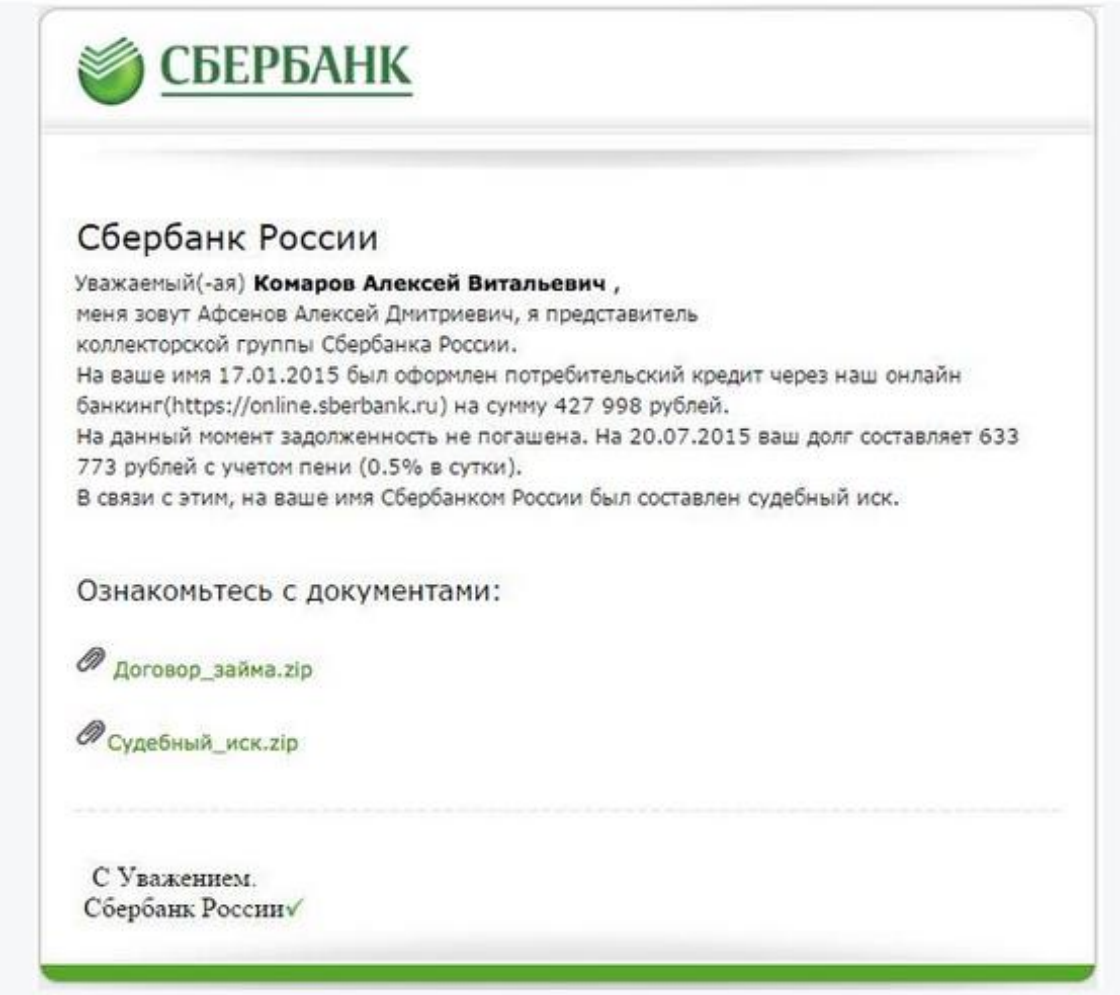

Рисунок 5. – Целенаправленное фишинговое почтовое сообщение с вложенными файлами

2. Сообщить человеку о радостной для него новости, например, что он выиграл крупную денежную сумму и может ее получить, но для этого необходимо, чтобы он сообщил идентификаторы своей банковской карты или оплатил перевод «выигранных» денежных средств (рисунок 7) (тактика «радости»). Получение внезапного подарка или приза всегда влияет на эмоциональное состояние человека, а также притупляет его критическое мышление. Подобная тактика является самой «древней» и носит наименование «нигерийских писем».

3. Послать сообщение пользователю электронной почты с некоторой интересной темой, в надежде на его любопытство (тактика «любопытства»). Любознательность человека является мишенью для эффективной реализации почтового фишинга. Грамотный выбор легенды сообщения (рисунок 8) и массовая его рассылка может дать возможность нарушителю скомпрометировать множество идентификаторов.

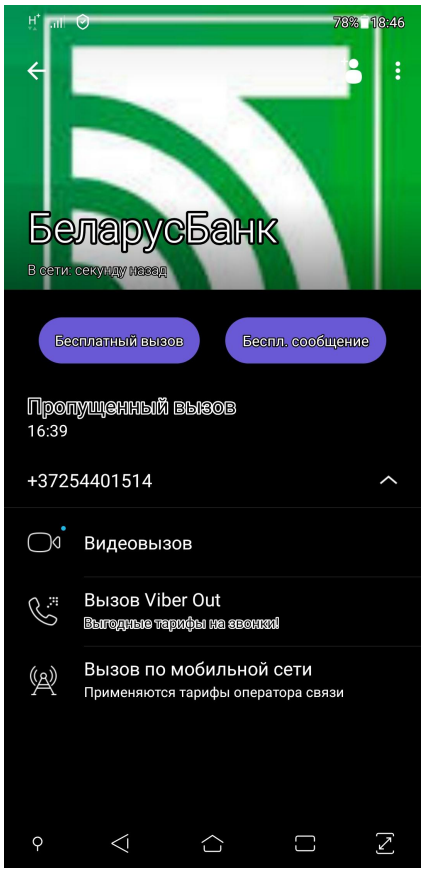

Рисунок 6. – Внешний вид мессенджера Viber используемого нарушителем

Рассмотрим признаки фишинга, которые можно обнаружить при анализе сообщений электронной почты. К ним мы будет относить отклонение от нормального положения дел. Таким образом, суть анализа сообщений – это обнаружение аномалий.

1. Отправитель сообщения и время его отправления

Отправитель может быть – известный или не известный (известных отправителей сложнее игнорировать). Время отправления сообщения может быть рабочее или не рабочее (деловая переписка в не рабочее время – может быть аномалией, так как многие люди редко задерживаются на работе для выполнения своих должностных обязанностей, откладывая то что не сделали сегодня на завтра).

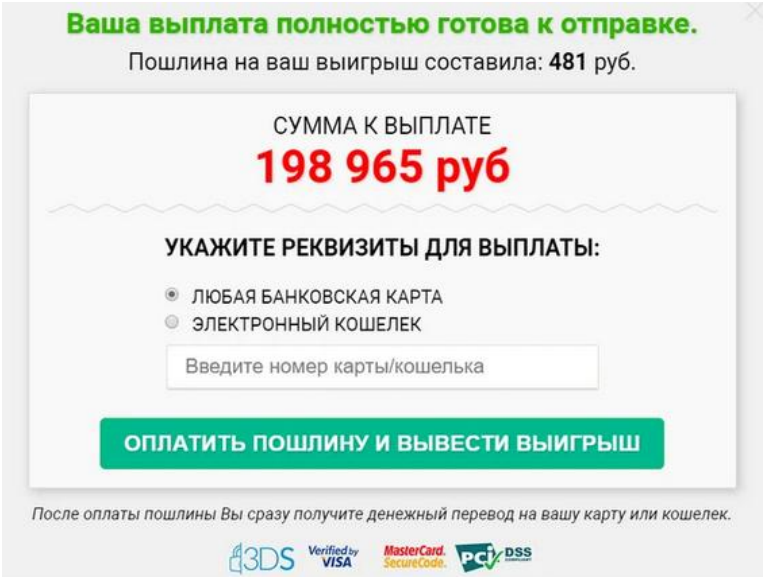

Рисунок 7. – Фишинговое почтовое сообщение о выигрыше

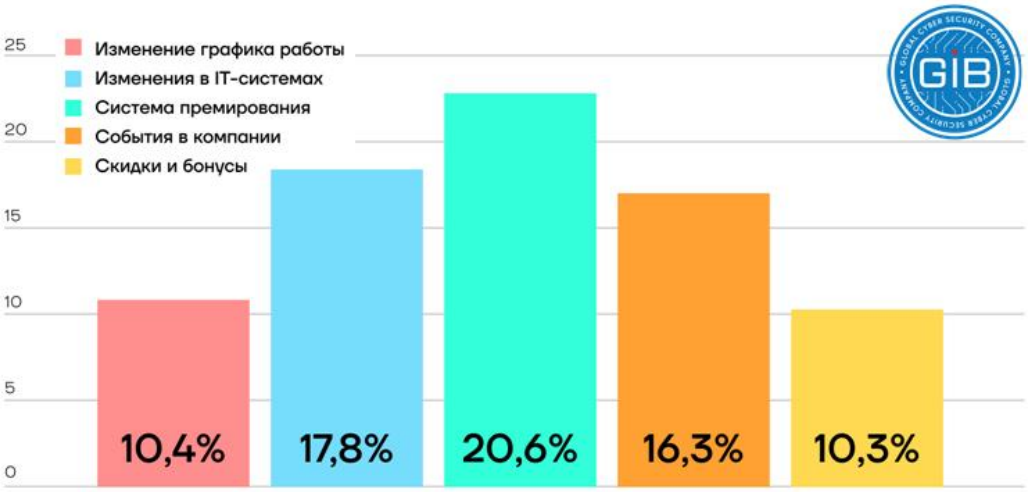

Рисунок 8. – Средняя результативность легенд сообщений электронной почты

2. Почтовый адрес отправителя сообщения

Необходимо обратить внимание на домен и наименование почтового ящика. Возможные аномалии: в результате анализа содержания сообщения делается вывод, что речь идет о деловой переписке, а для отправки сообщения используется не корпоративный домен электронной почты, а другие распространенные домены (например, mail.ru, gmail.com и т.д.). Наименование ящика электронной почты не содержит фамилии или имени отправителя сообщения (наличие фамилии, имени или инициалов в наименовании ящика – частый случай для корпоративной почты). Проверка принадлежности

домена (наименование ящика после символа «@») может быть реализована путем его введения в URL строку браузера. Это позволяет понять какая электронная почта, использовалась при отправке сообщения.

3. Текст сообщения и его оформление, тема сообщения

Текст сообщения должен отвечать требованиям деловой переписки не только по содержанию, но и оформлению. Признаки деловой переписки:

- приветственное обращение по имени и отчеству к адресату;
- ФИО отправителя, его должность и некоторые реквизиты организации.

4. Тип вложения

Возможные аномалии:

- вложение является архивом (*.rar, *.zip);
- вложение - гипертекстовая ссылка;
- вложение имеет не известное расширение (*.001) или двойное расширение (*.docx.exe).

5. Наименование вложения

Возможная аномалия: наименование файла представляет собой написание русского слова в транслитерации (Oplata.zip, Dokumenti_dlia_proverki.001).

Используя признаки фишинга, выполним анализ сообщения электронной почты (рисунок 9) и определим признаки фишинга. Исходные данные для анализа сообщения:

1. Сообщение получено преподавателем БГУИР на его корпоративную электронную почту.

2. Университет имеет корпоративную почту в домене bsuir.by.

1. Отправитель сообщения и время его отправления

Сообщение пришло от неизвестного для преподавателя лица. Время отправки – не рабочее, хотя судя по тексту сообщения, речь идет о деловой переписке.

Так как сообщение пришло не по назначению, то в данном случае нарушителем используется тактика «любопытства». Если такое сообщение было бы доставлено, сотруднику бухгалтерии, то тогда бы тактика была «страха», в виду того, что не оплата счетов вовремя ведет к проблемам у человека, не выполнившего такую должностную обязанность. Это умозаключение подтверждается содержанием сообщения, поэтому его текст имеет эмоциональную окраску побуждающую получателя к действию.

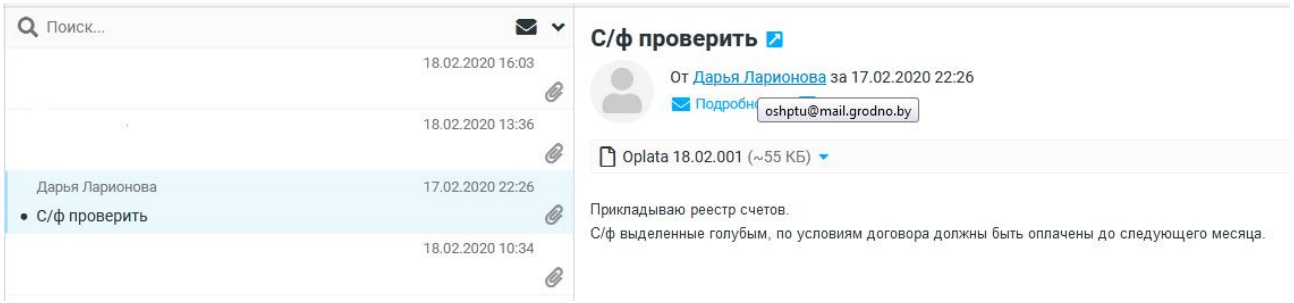

Рисунок 9. – Сообщение электронной почты

2. Почтовый адрес отправителя сообщения

Почтовый адрес отправителя сообщения: «oshptu@mail.grodno.by». Наименование почтового ящика «oshptu» не имеет ни чего общего с его отправителем «Дарьей Ларионовой». Домен, с которого отправлено письмо «mail.grodno.by» не имеет отношения к корпоративной почте конкретной организации. Этот сервис электронной почты предоставляется Белтелекомом, что подтверждается проверкой домена.

3. Текст сообщения и его оформление, тема сообщения

Текст сообщения имеет признаки деловой переписки, хотя в оформлении отсутствуют такие признаки. Тема письма «С/ф проверить» означает о том, что сообщение используется для пересылки счет-фактуры (сокращение С/ф). Преподаватель университета не является сотрудником бухгалтерии, поэтому счет-фактурами он не занимается. Исходя из чего, можно сделать вывод, что письмо пришло не по назначению. Кроме того, необходимо учесть, что случайностью пересылку сведений относящихся к информации ограниченного распространения (счет-фактура) назвать сложно.

Признаки управления действиями получателя сообщения присутствуют. Они реализуются через осмысление текста сообщения. Так например, для того чтобы оплатить счет- фактуру нужно ее открыть (открыть файл) или для того, чтобы полюбопытствовать, что находится в содержании счет-фактуры для этого нужно ее также открыть.

4. Тип вложения

К письму прикреплен файл, который имеет не известное расширение ***.**001, хотя речь идет о счет-фактуре, соответственно расширение файла должно соответствовать документам данной категории.

5. Наименование вложения

Вложением является файл с русским наименованием, написанным в транслитерации: Oplata 18.02.

Вывод: данное сообщение является фишинговым. Открытие файла приведет к запуску и установки вредоносной программы. Сообщение необходимо удалить.

2 Практическое задание

1. Проанализировать сообщение (см. Приложение), переданное по электронной почте и определить признаки фишинга в нем.
2. Составить фишинговое сообщение, в котором минимизировать признаки фишинга.

3 Контрольные вопросы

1. На чем основан фишинг?
2. В чем заключается сущность социальной инженерии?
3. Какой из видов фишинга наиболее опасный? Обоснуйте ответ.
4. Какой из видов фишинга наиболее эффективный для нарушителя? Обоснуйте ответ.
5. Какой из признаков фишинга наиболее оптимальный для обнаружения подобных сообщений? Обоснуйте ответ.

4 Приложение

Исходные данные: сообщение получено преподавателем БГУИР на его адрес корпоративной электронной почты. Домен БГУИР «bsuir.by».

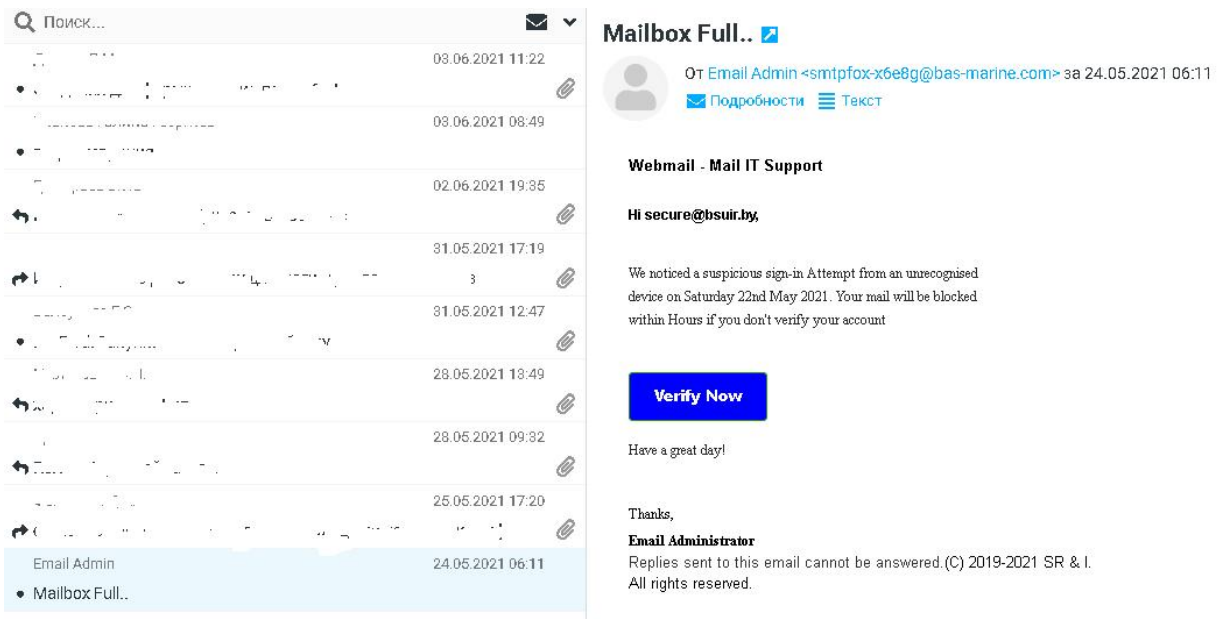

Рисунок 10. – Сообщение электронной почты