ЦЗИ ISC
INFORMATION SECURITY CENTER

ЦЕНТР ЗАЩИТЫ ИНФОРМАЦИИ
ГОСУДАРСТВЕННОГО ОБЪЕДИНЕНИЯ
«БЕЛОРУССКАЯ ЖЕЛЕЗНАЯ ДОРОГА»

ФИШИНГ

- Что такое фишинг
- Основные техники фишинга
- Признаки фишинга
- Примеры фишинга
- На что обращать внимание

Что такое фишинг

Фишинг (от английского fishing — рыбная ловля, выуживание)

Это вид **интернет-мошенничества**, целью которого является:

- **получение доступа к конфиденциальным данным пользователей** — логинам, паролям, данным кредитных карт, номерам телефонов, паспортным данным и другим чувствительным данным;
- **внедрение вредоносного программного обеспечения** в структуру организации для последующей её компрометации и взлома.

Основные техники фишинга

Фишинговая атака обычно осуществляется в форме сообщения, убеждающего Вас:

- Перейти по ссылке.
- Открыть документ.
- Установить приложения на устройство.
- Ввести имя пользователя и пароль на сайте, выглядящем вполне официально.

Признаки фишинговых писем

- В нем есть побуждение к немедленному действию. Пример: «Переходи сейчас, иначе приз заберет кто-то другой».
- Отсутствуют контактные данные отправителя.
- Описывается ситуация, к которой вы не имеете отношения. К примеру, погашение кредита, судебные тяжбы, банковские переводы.
- Ссылка выглядит нестандартно (случайный набор символов), тем более при наведении указателя мыши.

Признаки фишинговых писем

- Текст с замененными символами.
  Например: «Здравствуйте, Татьяна. В0сполbзуйтесь эт0й ссылk0й для в0сстановления пар0ля. 0на действителbна в течение 24 часов».
- Домен отправителя (якобы официального представителя) – не корпоративный, а обычный: mail.ru, gmail.com и так далее.
- Есть вложения со странными именами и расширением.
- Только картинки, QR-коды или кнопки.
- Запрос конфиденциальной или личной информации.
- Призыв скачать файл.

Примеры фишинговых писем

Тема письма отправителя не носит рабочий характер

Обратить внимание на вложенный файл

Текст письма имеет эмоциональный окрас.

IFC Global Development Program <postmaster@equibowen.com>

You've Won US $5,000,000 in the IFC Global Development Funding.

DHL_FORM_20230203.PDF.zip
183 KB

Congratulations! You have been selected as the winner of US$5,000,000 in the IFC Global Development Funding Program.
We are delighted to inform you that your Email & Name was luckily selected among the recipient of US$5,000,000 in this year's 2023 IFC Development Fundung. This program aims to provide strong finance for global development and support for people to promote life and the environment. With this funding, we believe you will be able to make significant progress in your work to improve the lives of those around you.

Your Ticket number is IFCW276/2712. All participants were selected through a computer-random integrated system drawn from millions of E-mail addresses via the Internet and lucky winners do not have to purchase any tickets to participate in this program.
Consequently, you have been certified to receive a payout of Five Million United States Dollars (US$5,000,000.00) from the IFC Funding program.

For the processing of your payment Contact: Mr. John Gandolfo
Treasury & Mobilization Officer
1st E-mail: cssdept@accountant.com
2nd E-mail: cssdept@accountant.com
WhatsApp: +1 209 683-4288
Tel: +44 740 117-4240

Фишинговая ссылка

Note: This Program is sponsored and organized by the International Finance Corporation (IFC) a member of the World Bank Group.
~ Further information about this program and a list of the selected recipients for 2023 will always be published in UK Metro NewsPaper, Daily Telegraph UK, Business Guide Magazine, and Newsletters.

Yours in service,
Mr. Steven Shalita

Communications & Outreach ®
****

Указан не полный адрес отправителя

NOTE: If you received this message in your SPAM/BULK folder, that is because of the restrictions implemented by your Internet Service Provider, we urge you to follow it up with utmost commitment for a positive result.

DHL Express Services <jane@telonuevo.com> | yyqxxb@cma.gov.cn

Re: Your DHL Parcel Just Arrived - AWB:13285643468

Чтобы скачать рисунки, щелкните эту ссылку. Автоматическое скачивание некоторых рисунков в Outlook было отменено в целях защиты конфиденциальности личных данных.

DHL Receipt_pdf.rar
416 KB

Обратить внимание на вложенный файл

Текст письма носит не деловой характер

Dear Valued Customer,

Your Shipping Documents are on the way .

Find attached DHL Receipt to track your shipment or make some changes.

DELIVERY INFORMATION

Waybill No.	13285643468
Delivery status	On Transit
Scheduled Delivery Date	Wednesday May 17 2023
Delivery Time	End of the day

Thank you for using Dhl Delivery.

DHL Express - Excellence. Simply delivered.

Обратить внимание на вложенный файл

Осуществлена подмена адресов с преобразованием в ссылку

usraju <admpoezd@mnsk.rw.by> admpoezd@mnsk.rw.by

Purchase Order PO20230305

PO20230305.doc
25 KB

Good morning: admpoezd@mnsk.rw.by

I trust that all is well with you. Please find attached Purchase Order PO20230305 dated 03/05/2023.

Please confirm that the prices, etc. are in order. the prices are based on your last price list issued at the exh
As we have not been in contact for a while, kindly make corrections if need be and send us a proforma invo

N.B. Please acknowledge receipt and acceptance of order by return e-mail within 2 working days.
refer this email to the appropriate department for immidate attention

Should you have any queries, please do not hesitate to contact me.

Kind Regards,
USRAJU (PPIC)
Phone No.: 8897700078.
Seutic Group

Адрес электронной почты не относится к корпоративной БЖД

Rana <rana@ckegroup.net> nod1@mnsk.rw.by

SP24 Invoice

SP24_Invoice.xls
269 KB

Обратить внимание на вложенный файл

Resending!

Good morning,

Please find the invoice attached.

Rana

Tinkoff Ivest Тимур Камронович <info@inlavka.ru>

Re: Срочно. Не упустите возможность получать стабильный доход ежедневно с нами.

В Этом Файле Находится Приглашение, Которое Может Быть Важным Для Вас-YdQ7PUs0383263.pdf
85 KB

Тема письма носит побуждающий характер

Инвестируйте умно с помощью Тинькофф Инвестиции

Тимошку Анна <sroojhvupby@finzachet.ru> inysik@rw.by

Re:Важная информация.

ПЕРСОНАЛЬНОЕ ИНВЕСТИЦИОННОЕ ПРИГЛАШЕНИЕ ДОСТУПНО В ПРИЛОЖЕННОМ ФАЙЛЕ-ePx3AOnRf81174.pdf
36 KB

Название файла носит побуждающий характер

Имя файла: ПЕРСОНАЛЬНОЕ ИНВЕСТИЦИОННОЕ ПРИГЛАШЕНИЕ ДОСТУПНО В ПРИЛОЖЕННОМ ФАЙЛЕ-ePx3AOnRf81174.pdf
Тип файла: .pdf-файл
Размер файла: 36 Кбайт

Мы были бы рады видеть вас в нашей команде нового проекта от Тинькофф Банка Инвестиции в ка

Личное приглашение в наш проект уже готово и доступно в прикрепленном файле. Присоединитесь к нам и работайте в команде профессионалов над инновационными проектами.

Purchasing <purchasing.exe@qson.com.sg> ns@nw.by

order

QUOTE-272.z
518 KB

Dear Sir,

Kindly give me your best price and stock availability for the following as attached.

If got any lead time please specify. Also, please provide certification.

Look forward to your kind offer.

Thanks & regards
Annie Chung
Purchasing Department
Q'Son Kitchen Equipment Pte Ltd
Block 115 A Commonwealth Drive #01-27/28
Singapore 149596
Tel: 6472 7337 Fax: 6472 6497
Email: purchasing.exe@qson.com.sg
Web: www.qson.com.sg

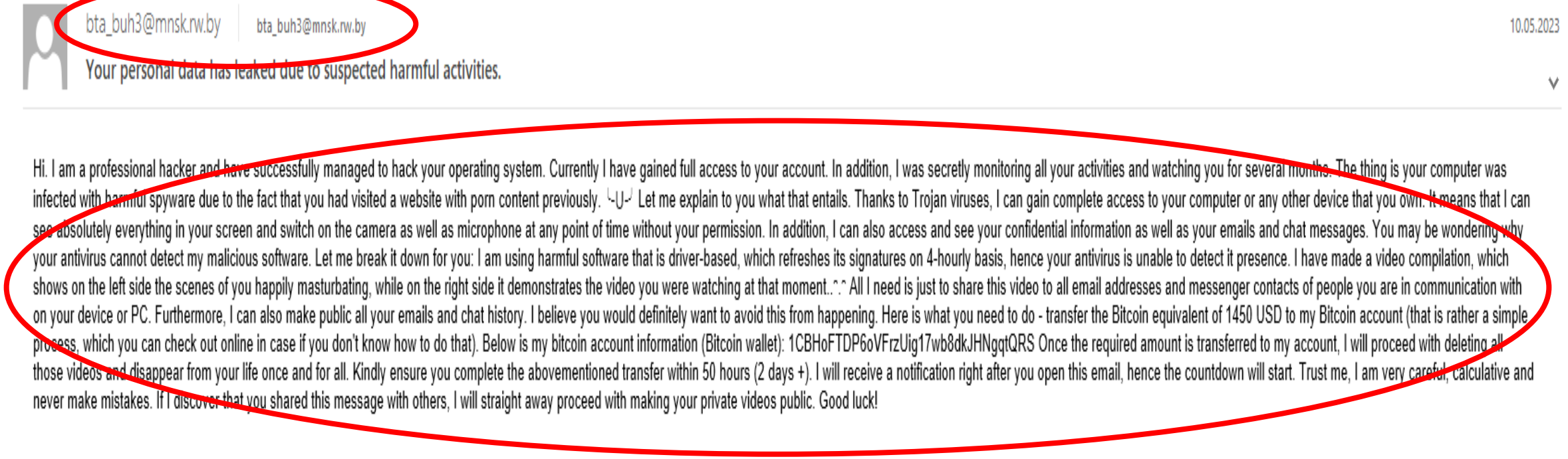
Представлены реквизиты организации под видом официальных с фишинговой ссылкой

Содержит QR-код для сканирования

Android IOS

Один и тот же адрес отправителя и получателя

Письмо содержит угрозу взлома и попытку шантажа с целью получения выкупа.

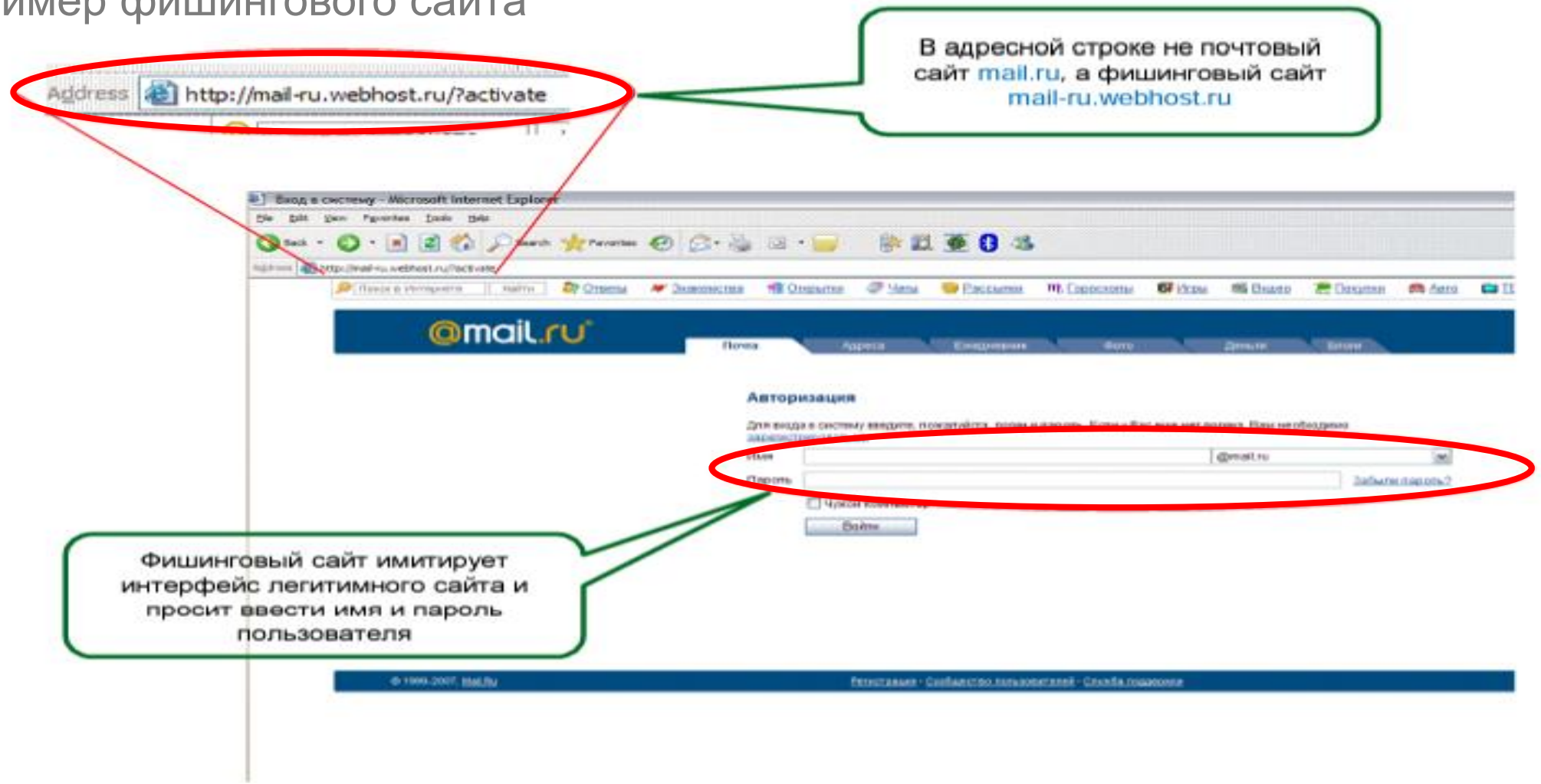


bta_buh3@mnsk.rw.by bta_buh3@mnsk.rw.by 10.05.2023

Your personal data has leaked due to suspected harmful activities.

Hi. I am a professional hacker and have successfully managed to hack your operating system. Currently I have gained full access to your account. In addition, I was secretly monitoring all your activities and watching you for several months. The thing is your computer was infected with harmful spyware due to the fact that you had visited a website with porn content previously. ╰(U)╯ Let me explain to you what that entails. Thanks to Trojan viruses, I can gain complete access to your computer or any other device that you own. It means that I can see absolutely everything in your screen and switch on the camera as well as microphone at any point of time without your permission. In addition, I can also access and see your confidential information as well as your emails and chat messages. You may be wondering why your antivirus cannot detect my malicious software. Let me break it down for you: I am using harmful software that is driver-based, which refreshes its signatures on 4-hourly basis, hence your antivirus is unable to detect it presence. I have made a video compilation, which shows on the left side the scenes of you happily masturbating, while on the right side it demonstrates the video you were watching at that moment..^.^ All I need is just to share this video to all email addresses and messenger contacts of people you are in communication with on your device or PC. Furthermore, I can also make public all your emails and chat history. I believe you would definitely want to avoid this from happening. Here is what you need to do - transfer the Bitcoin equivalent of 1450 USD to my Bitcoin account (that is rather a simple process, which you can check out online in case if you don't know how to do that). Below is my bitcoin account information (Bitcoin wallet): 1CBHoFTDP6oVFrzUig17wb8dkJHNgqtQRS Once the required amount is transferred to my account, I will proceed with deleting all those videos and disappear from your life once and for all. Kindly ensure you complete the abovementioned transfer within 50 hours (2 days +). I will receive a notification right after you open this email, hence the countdown will start. Trust me, I am very careful, calculative and never make mistakes. If I discover that you shared this message with others, I will straight away proceed with making your private videos public. Good luck!

Пример фишингового сайта



На что обращать внимание

Отправитель, время	Отправитель – известный / **не известный** (известных отправителей сложнее игнорировать). Время рабочее / **не рабочее** (деловая переписка в не рабочее время – может быть аномалией)
Почтовый адрес отправителя	Домен и наименование почтового ящика. **Возможные аномалии:** деловая переписка – бесплатный домен. Наименование ящика не содержит фамилии или имени отправителя

На что обращать внимание

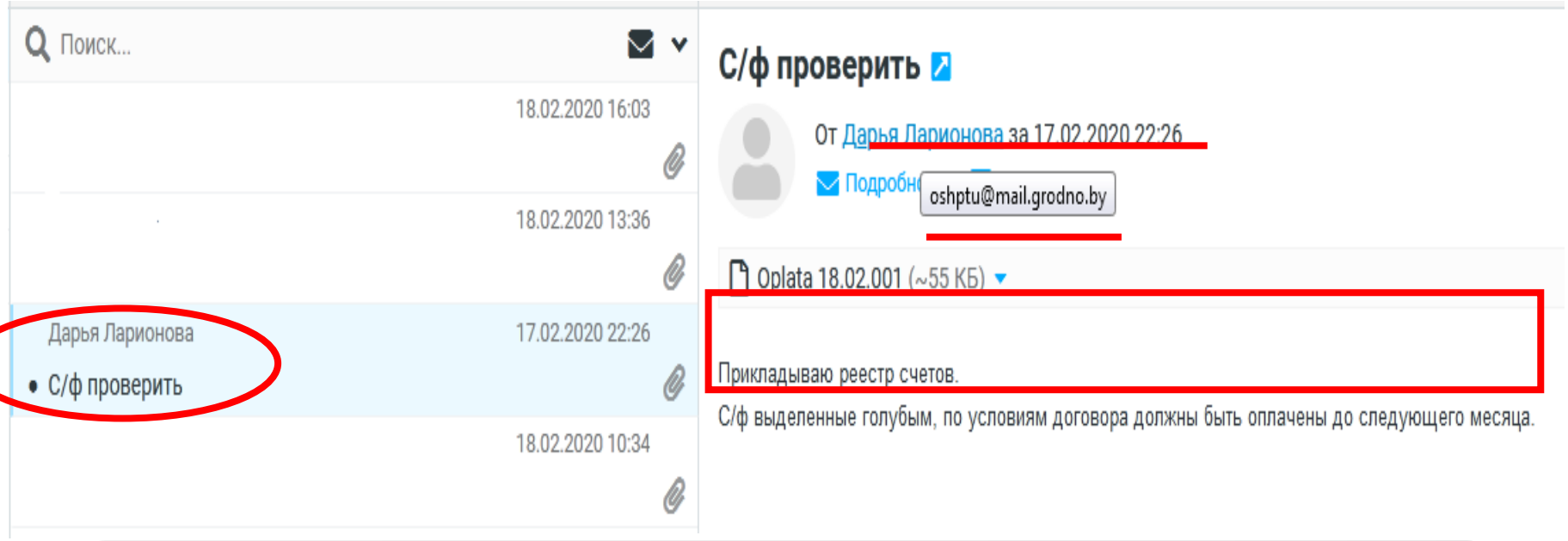
Текст письма, его тема и оформление

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

Признаки деловой переписки

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

На что обращать внимание



Признаки фишинга

1. Контекст письма, говорит о том что оно пришло не по назначению;
2. Текст письма имеет эмоциональную окраску;
3. Есть признаки управления действиями получателя

На что обращать внимание

Тип вложения

Возможные аномалии:

1. Архив (*.rar, *.zip);
2. Гипертекстовая ссылка;
3. Вложение имеет не известное расширение (*.001) или двойное расширение (*.docx.exe)

Наименование вложения

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

На что обращать внимание

Имя почтового ящика и домена (примеры)

1. belarusbank@yandex.by → belarusbak@yandex.by
2. info@belarusbank.by → belarusbank@yandex.by
3. isc@isc.by → lsc@isc.by

1. Описка в виде одной пропущенной буквы
2. Домен не корпоративный
3. Комбинации слов с латинскими буквами i и l

Рекомендации пользователю

- внимательно проверяйте имя и домен, с которого отправляется электронное письмо: большинство писем от легитимных компаний не приходит с почты gmail.com, live.com и т. д. Обычно официальные письма приходят с частных доменов;
- проверьте наличие явных орфографических ошибок в теме и тексте сообщения;
- обезличенные поля «От» и «Кому» могут быть признаком фишинга;
- не сообщайте свои учетные данные — законные отправители никогда их не попросят;
- не открывайте вложения и не загружайте подозрительные ссылки;
- используйте в рабочей переписке только служебную почту;
- не указывайте рабочую почту на сторонних ресурсах.

Руководство к действию

При подозрении на то, что полученное письмо — фишинговое, не открывайте какие-либо вложения и не переходите по ссылкам.

Вместо этого отметьте его и сообщите

системному администратору, либо работнику, ответственному за информационную безопасность в вашем подразделении!!!

** Приведенные в презентации примеры фишинговых писем взяты из сети Белорусской железной дороги*

Помните!

Для достижения своих целей злоумышленники **могут использовать разные способы** для получения интересующей их информации, в том числе методы социальной инженерии. Как правило, телефон. Вам звонят из банка и просят подтвердить перевод денег, который вы, естественно, не совершали В итоге вы сами, добровольно сообщаете свои данные карты, CVV-код и иные сведения, с помощью которых потом можно провести реальную операцию по снятию и переводу наличных.

Или, к примеру, вам звонят и представляются сотрудниками государственных органов и просят сообщить конфиденциальную информацию о Вас или Ваших близких.

Вместе с тем, **злоумышленники могут уже обладать конфиденциальной информацией о Вас или Ваших коллегах**, заполучив ее неправомерно из других источников (соц. сети, дисконтные карточки и т.д.), чем могут ввести вас в заблуждение и выманить интересующую их информацию.

Ни в коем случае не сообщайте данные о вашей работе, Вас и Ваших близких по телефону!!!