ЕВРАЗ

Код ИБ.
Безопасная среда.

Как научить сотрудников выявлять фишинг. Кейсы из практики.

Нуйкин Андрей

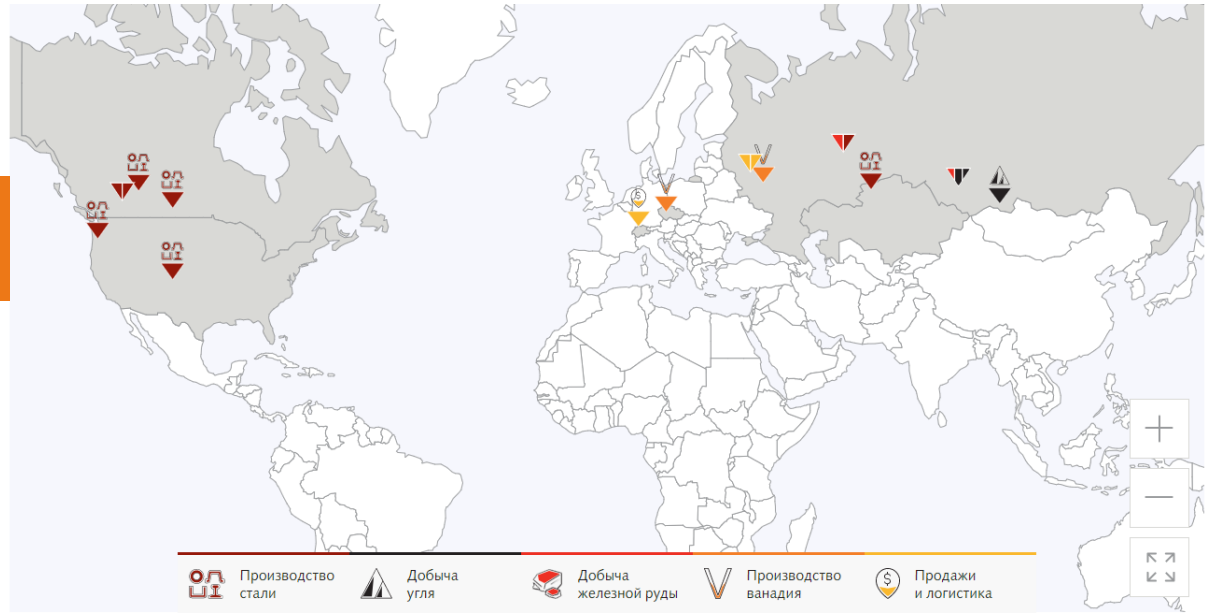
11.11.2020

Что такое ЕВРАЗ?

ЕВРАЗ

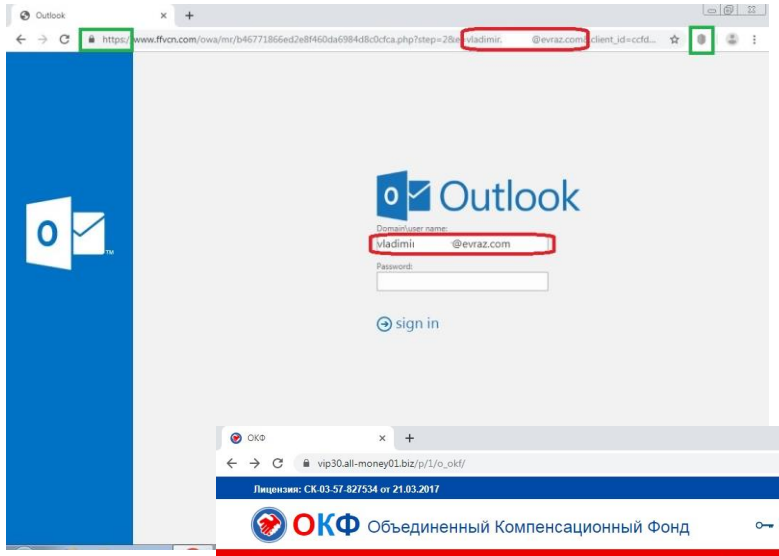
- ГЛОБАЛЬНАЯ ГОРНО-МЕТАЛЛУРГИЧЕСКАЯ КОМПАНИЯ

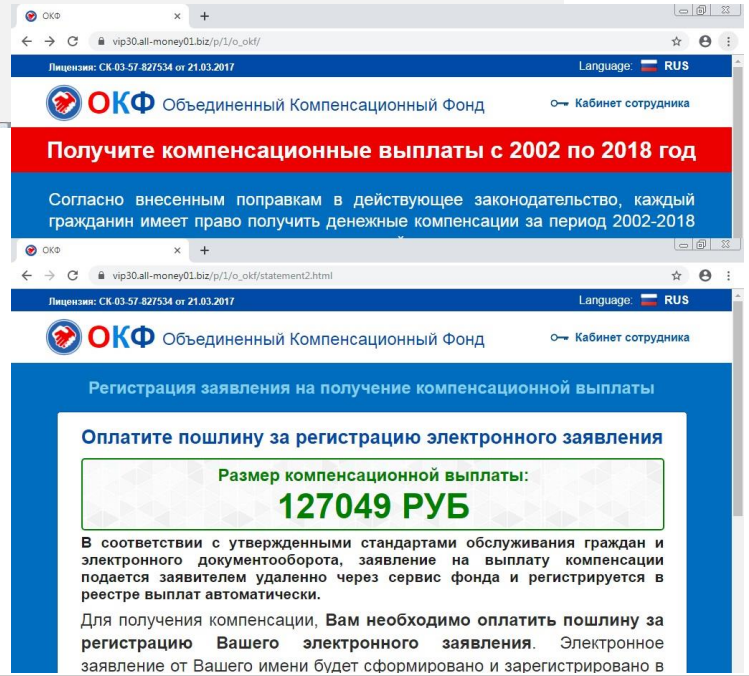
ЕВРАЗ является вертикально-интегрированной металлургической и горнодобывающей компанией с активами в России, США, Канаде и Казахстане. Компания входит в число крупнейших производителей стали в мире. Собственная база железной руды и коксующегося угля практически полностью обеспечивает внутренние потребности ЕВРАЗа. Компания входит в ведущий индекс Лондонской Фондовой Биржи FTSE-100.

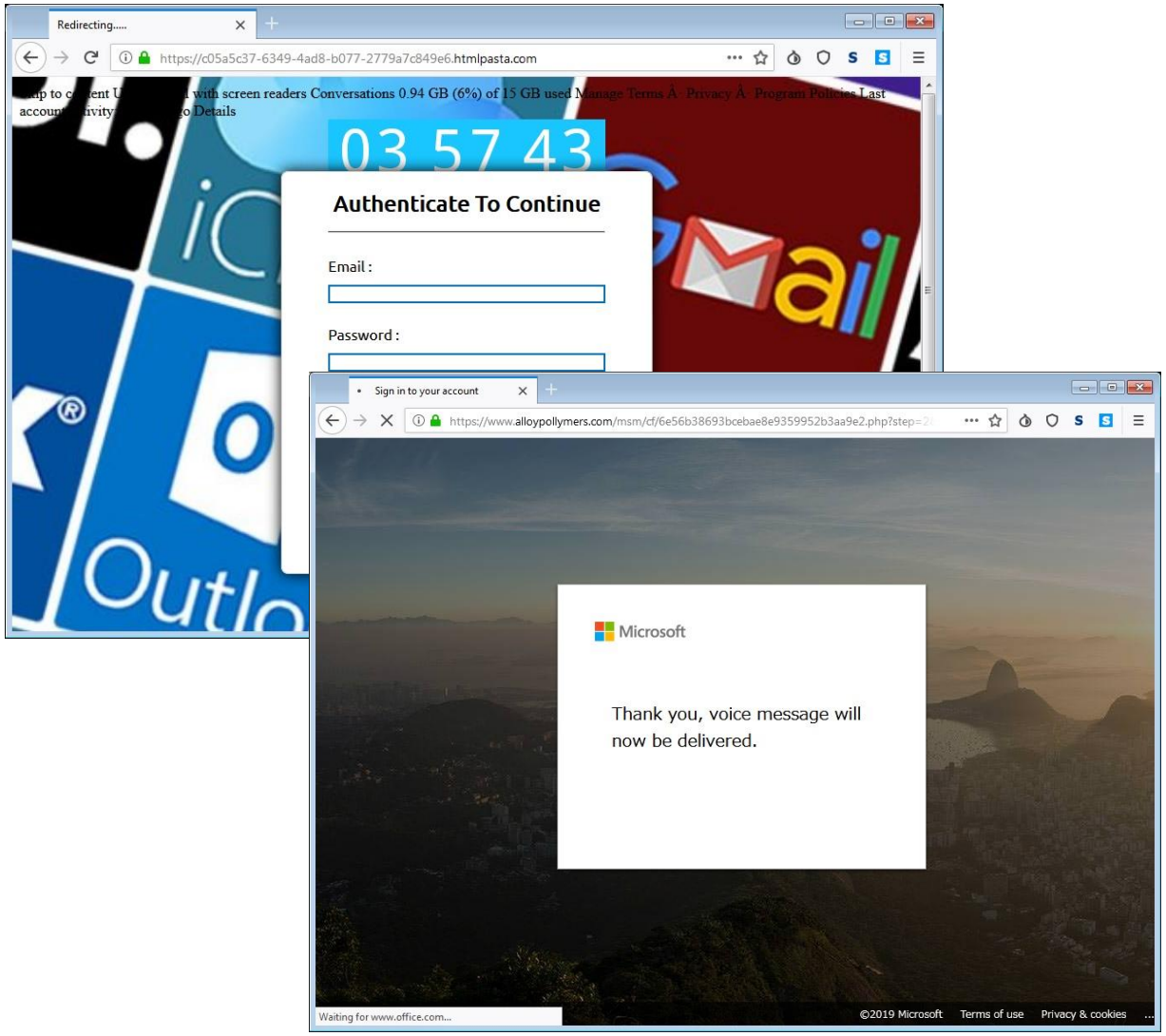


Предпосылки для проведений учений

ЕВРАЗ

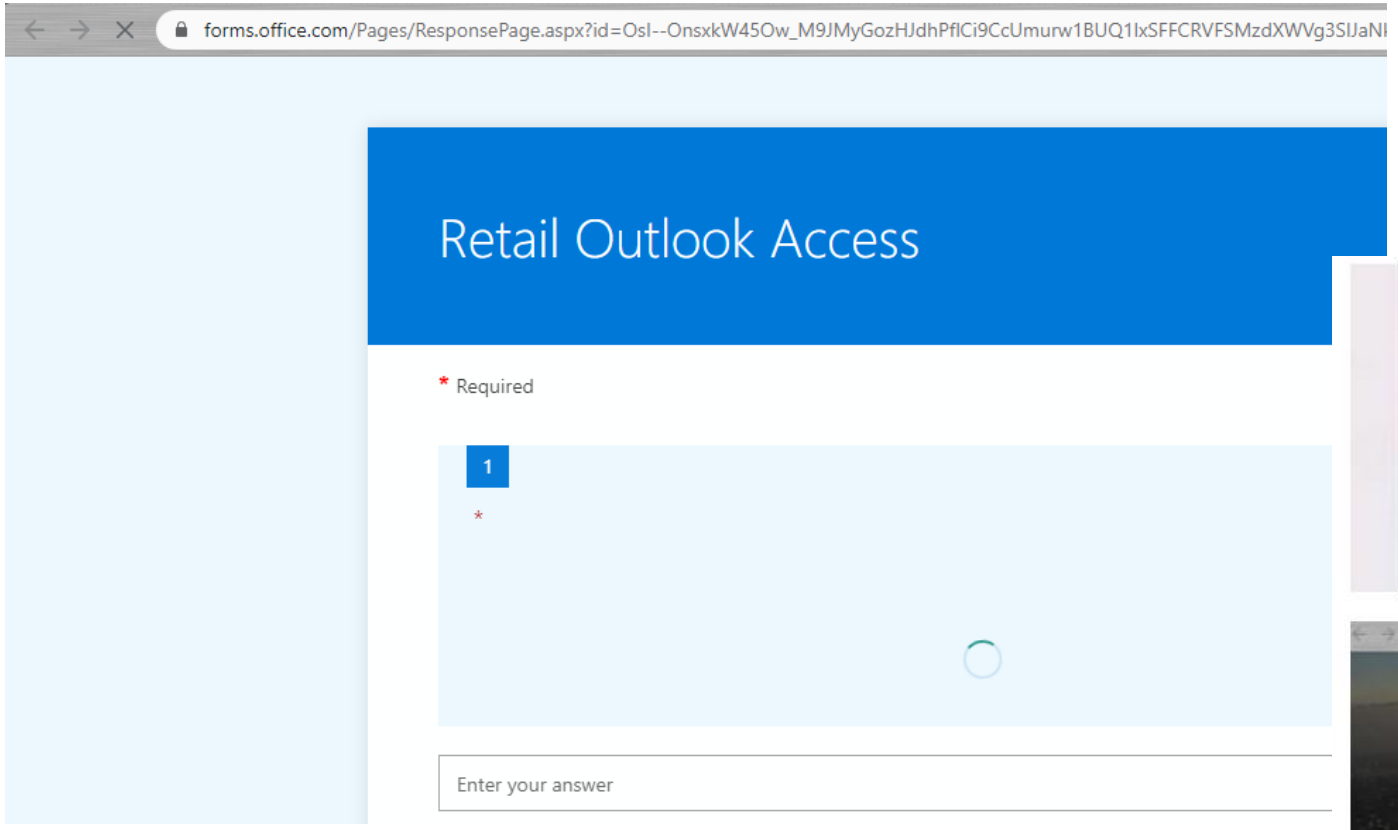


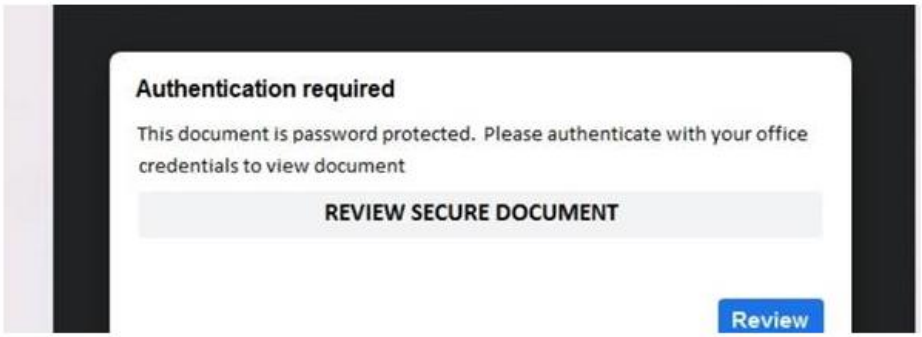


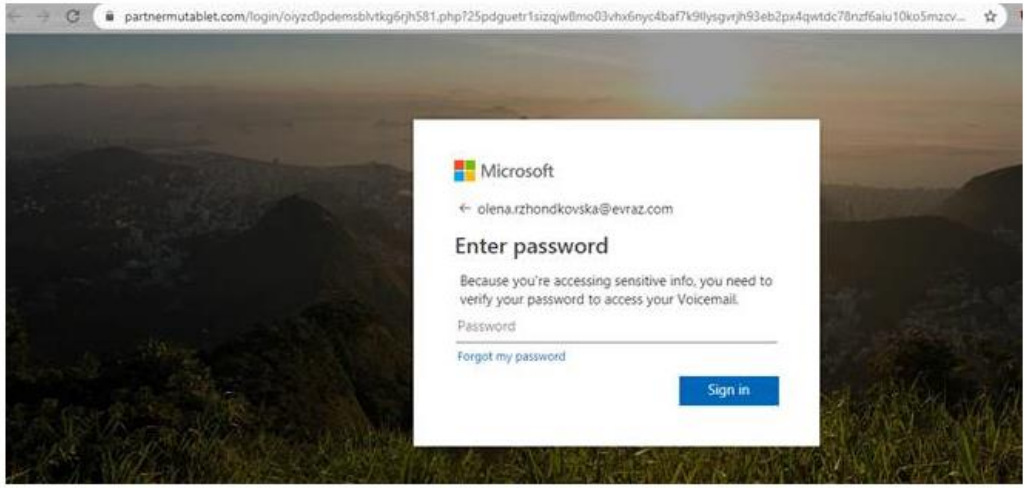


Предпосылки для проведений учений

ЕВРАЗ

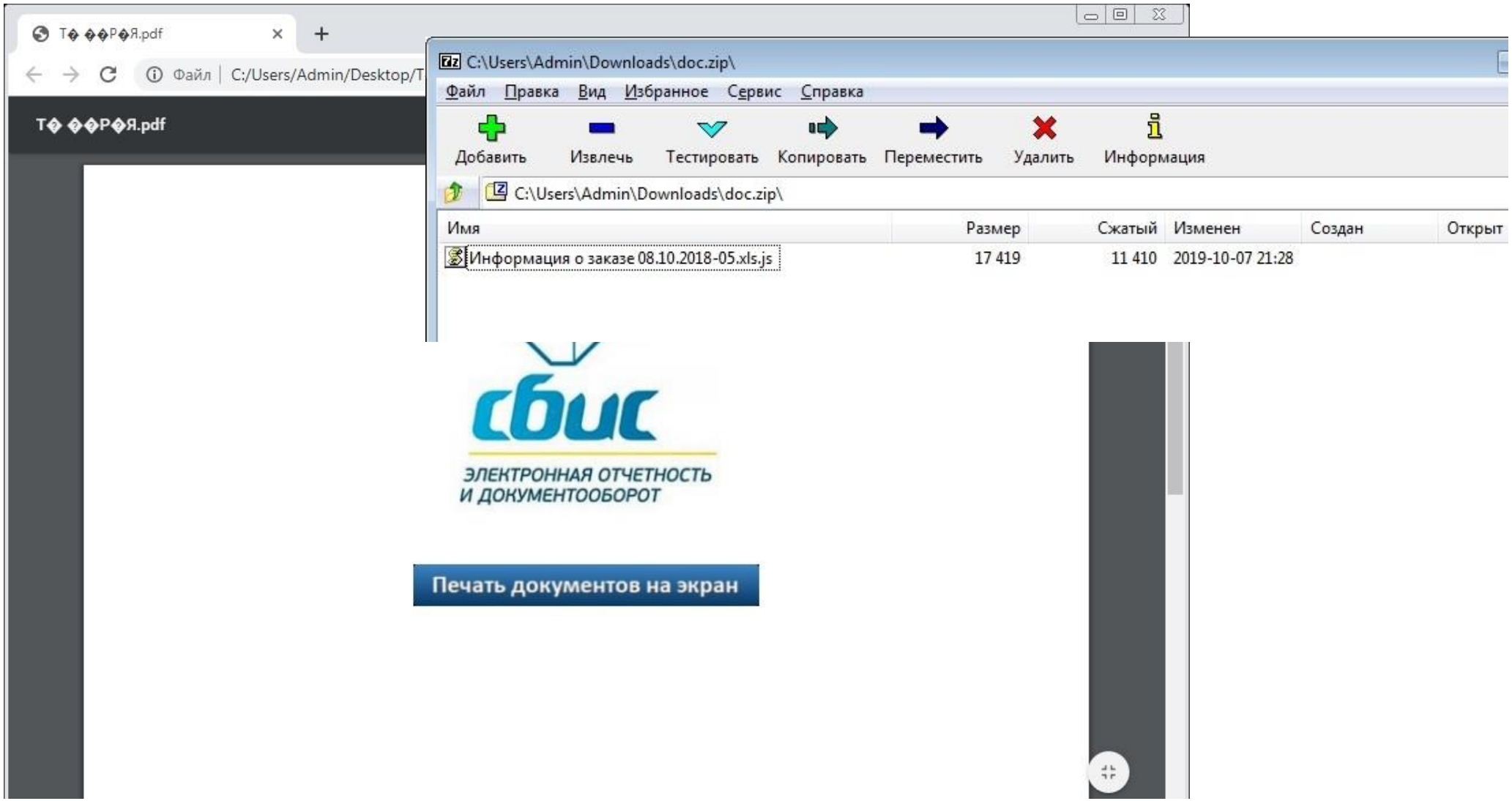






Предпосылки для проведений учений

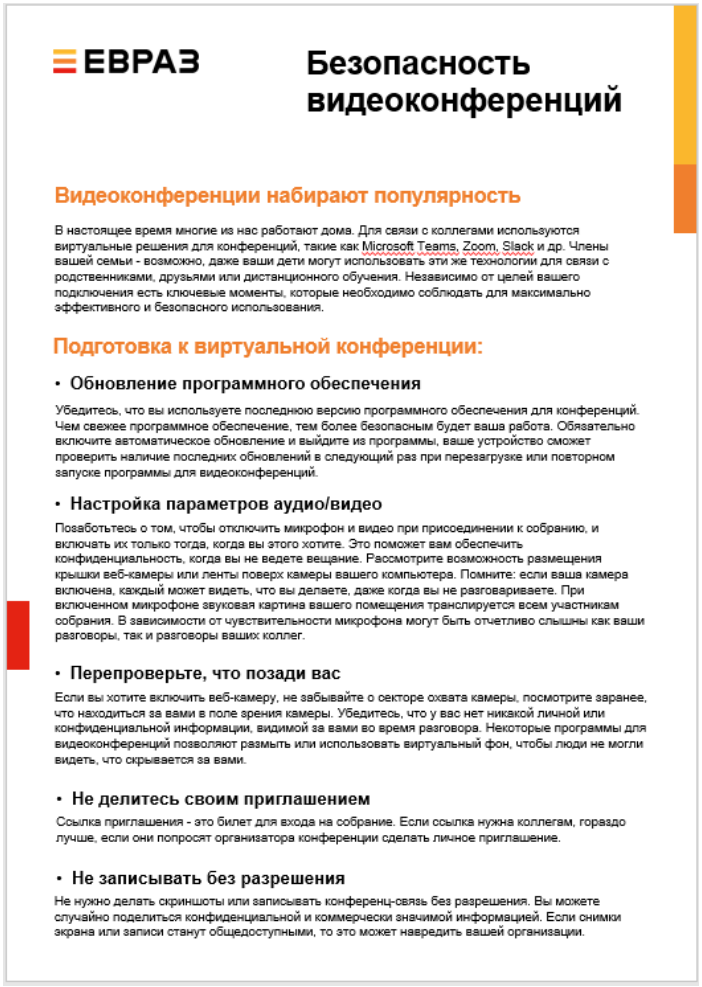
ЕВРАЗ



Что делаем в целом

ЕВРАЗ

Ежемесячный вестник ИБ



ЕВРАЗ

Безопасность видеоконференций

Видеоконференции набирают популярность

В настоящее время многие из нас работают дома. Для связи с коллегами используются виртуальные решения для конференций, такие как Microsoft Teams, Zoom, Slack и др. Члены вашей семьи - возможно, даже ваши дети могут использовать эти же технологии для связи с родственниками, друзьями или дистанционного обучения. Независимо от целей вашего подключения есть ключевые моменты, которые необходимо соблюдать для максимально эффективного и безопасного использования.

Подготовка к виртуальной конференции:

- **Обновление программного обеспечения**

Убедитесь, что вы используете последнюю версию программного обеспечения для конференций. Чем свежее программное обеспечение, тем более безопасным будет ваша работа. Обязательно включите автоматическое обновление и выйдите из программы, ваше устройство сможет проверить наличие последних обновлений в следующий раз при перезагрузке или повторном запуске программы для видеоконференций.

- **Настройка параметров аудио/видео**

Позаботьтесь о том, чтобы отключить микрофон и видео при присоединении к собранию, и включать их только тогда, когда вы этого хотите. Это поможет вам обеспечить конфиденциальность, когда вы не ведете вещание. Рассмотрите возможность размещения крышки веб-камеры или ленты поверх камеры вашего компьютера. Помните: если ваша камера включена, каждый может видеть, что вы делаете, даже когда вы не разговариваете. При включенном микрофоне звуковая картина вашего помещения транслируется всем участникам собрания. В зависимости от чувствительности микрофона могут быть отчетливо слышны как ваши разговоры, так и разговоры ваших коллег.

- **Перепроверьте, что позади вас**

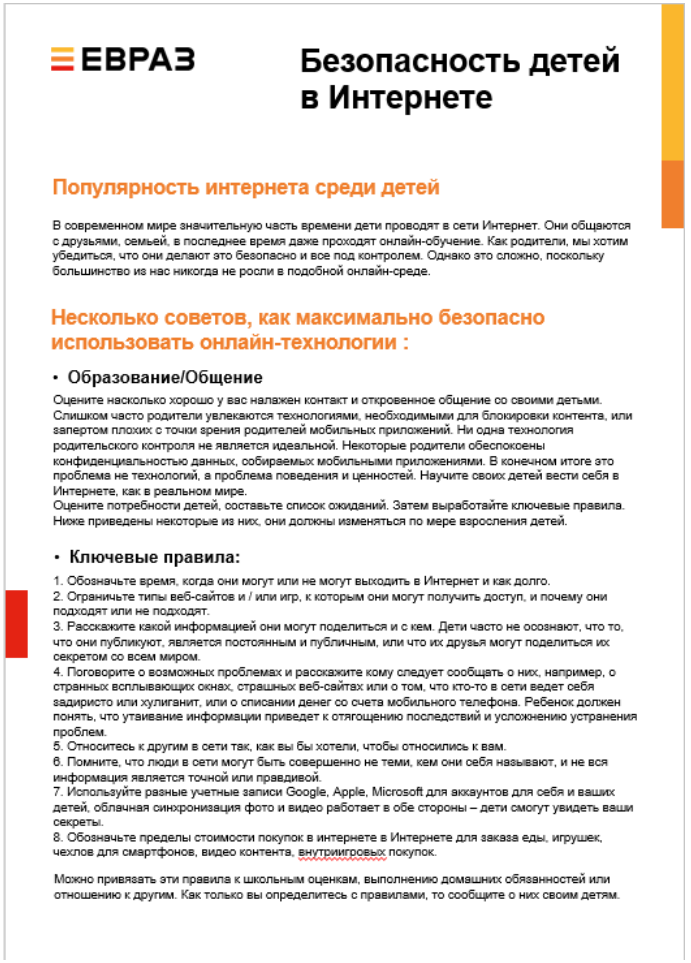
Если вы хотите включить веб-камеру, не забывайте о секторе охвата камеры, посмотрите заранее, что находиться за вами в поле зрения камеры. Убедитесь, что у вас нет никакой личной или конфиденциальной информации, видимой за вами во время разговора. Некоторые программы для видеоконференций позволяют размыть или использовать виртуальный фон, чтобы люди не могли видеть, что скрывается за вами.

- **Не делитесь своим приглашением**

Ссылка приглашения - это билет для входа на собрание. Если ссылка нужна коллегам, гораздо лучше, если они попросят организатора конференции сделать личное приглашение.

- **Не записывать без разрешения**

Не нужно делать скриншоты или записывать конференц-связь без разрешения. Вы можете случайно поделиться конфиденциальной и коммерчески значимой информацией. Если снимки экрана или записи станут общедоступными, то это может навредить вашей организации.



ЕВРАЗ

Безопасность детей в Интернете

Популярность интернета среди детей

В современном мире значительную часть времени дети проводят в сети Интернет. Они общаются с друзьями, семьей, в последнее время даже проходят онлайн-обучение. Как родители, мы хотим убедиться, что они делают это безопасно и все под контролем. Однако это сложно, поскольку большинство из нас никогда не росли в подобной онлайн-среде.

Несколько советов, как максимально безопасно использовать онлайн-технологии :

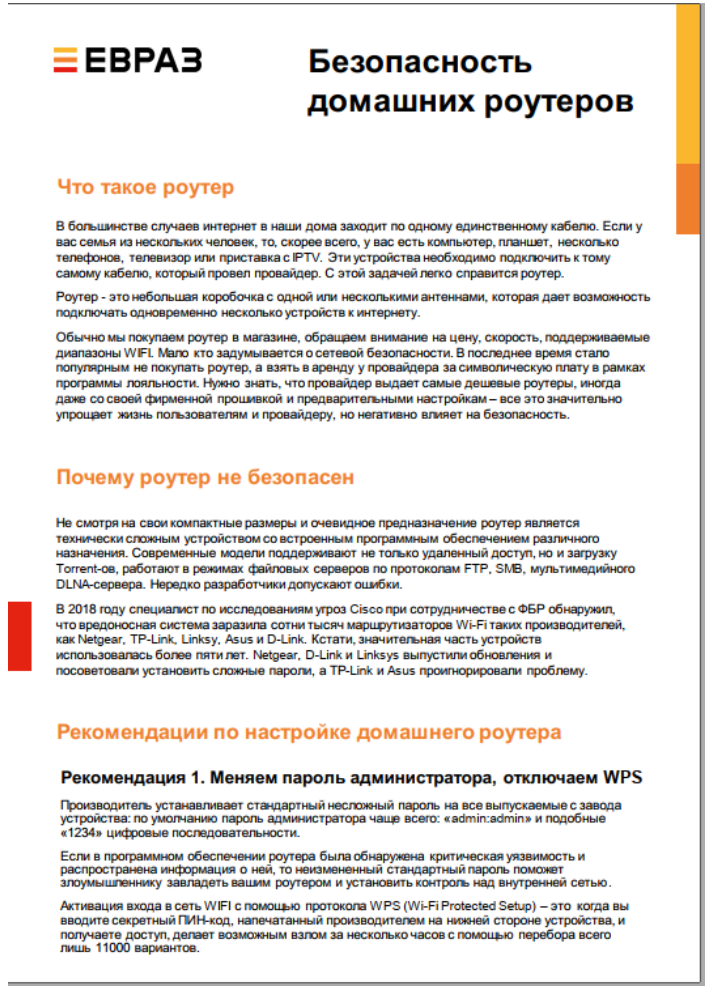
- **Образование/Общение**

Оцените насколько хорошо у вас налажен контакт и откровенное общение со своими детьми. Слишком часто родители увлекаются технологиями, необходимыми для блокировки контента, или запертом плохих с точки зрения родителей мобильных приложений. Ни одна технология родительского контроля не является идеальной. Некоторые родители обеспокоены конфиденциальностью данных, собираемых мобильными приложениями. В конечном итоге это проблема не технологий, а проблема поведения и ценностей. Научите своих детей вести себя в Интернете, как в реальном мире.
Оцените потребности детей, составьте список ожиданий. Затем выработайте ключевые правила. Ниже приведены некоторые из них, они должны изменяться по мере взросления детей.

- **Ключевые правила:**

1. Обозначьте время, когда они могут или не могут выходить в Интернет и как долго.
2. Ограничьте типы веб-сайтов и / или игр, к которым они могут получить доступ, и почему они подходят или не подходят.
3. Расскажите какой информацией они могут поделиться и с кем. Дети часто не осознают, что то, что они публикуют, является постоянным и публичным, или что их друзья могут поделиться их секретом со всем миром.
4. Поговорите о возможных проблемах и расскажите кому следует сообщать о них, например, о странных всплывающих окнах, страшных веб-сайтах или о том, что кто-то в сети ведет себя задиристо или хулиганит, или о списании денег со счета мобильного телефона. Ребенок должен понять, что утаивание информации приведет к отягощению последствий и усложнению устранения проблем.
5. Относитесь к другим в сети так, как вы бы хотели, чтобы относились к вам.
6. Помните, что люди в сети могут быть совершенно не теми, кем они себя называют, и не вся информация является точной или правдивой.
7. Используйте разные учетные записи Google, Apple, Microsoft для аккаунтов для себя и ваших детей, облачная синхронизация фото и видео работает в обе стороны – дети смогут увидеть ваши секреты.
8. Обозначьте пределы стоимости покупок в интернете в Интернете для заказа еды, игрушек, чехлов для смартфонов, видео контента, внутриигровых покупок.

Можно привязать эти правила к школьным оценкам, выполнению домашних обязанностей или отношению к другим. Как только вы определитесь с правилами, то сообщите о них своим детям.



ЕВРАЗ

Безопасность домашних роутеров

Что такое роутер

В большинстве случаев интернет в наши дома заходит по одному единственному кабелю. Если у вас семья из нескольких человек, то, скорее всего, у вас есть компьютер, планшет, несколько телефонов, телевизор или приставка с IPTV. Эти устройства необходимо подключить к тому самому кабелю, который провел провайдер. С этой задачей легко справится роутер.

Роутер - это небольшая коробочка с одной или несколькими антеннами, которая дает возможность подключать одновременно несколько устройств к интернету.

Обычно мы покупаем роутер в магазине, обращаем внимание на цену, скорость, поддерживаемые диапазоны WIFI. Мало кто задумывается о сетевой безопасности. В последнее время стало популярным не покупать роутер, а взять в аренду у провайдера за символическую плату в рамках программы лояльности. Нужно знать, что провайдер выдает самые дешевые роутеры, иногда даже со своей фирменной прошивкой и предварительными настройкам – все это значительно упрощает жизнь пользователям и провайдеру, но негативно влияет на безопасность.

Почему роутер не безопасен

Не смотря на свои компактные размеры и очевидное предназначение роутер является технически сложным устройством со встроенным программным обеспечением различного назначения. Современные модели поддерживают не только удаленный доступ, но и загрузку Torrent-ов, работают в режимах файловых серверов по протоколам FTP, SMB, мультимедийного DLNA-сервера. Нередко разработчики допускают ошибки.

В 2018 году специалист по исследованиям угроз Cisco при сотрудничестве с ФБР обнаружил, что вредоносная система заразила сотни тысяч маршрутизаторов Wi-Fi таких производителей, как Netgear, TP-Link, Linksy, Asus и D-Link. Кстати, значительная часть устройств использовалась более пяти лет. Netgear, D-Link и Linksys выпустили обновления и посоветовали установить сложные пароли, а TP-Link и Asus проигнорировали проблему.

Рекомендации по настройке домашнего роутера

Рекомендация 1. Меняем пароль администратора, отключаем WPS

Производитель устанавливает стандартный несложный пароль на все выпускаемые с завода устройства: по умолчанию пароль администратора чаще всего: «admin:admin» и подобные «1234» цифровые последовательности.

Если в программном обеспечении роутера была обнаружена критическая уязвимость и распространена информация о ней, то неизмененный стандартный пароль поможет злоумышленнику завладеть вашим роутером и установить контроль над внутренней сетью.

Активация входа в сеть WIFI с помощью протокола WPS (Wi-Fi Protected Setup) – это когда вы вводите секретный ПИН-код, напечатанный производителем на нижней стороне устройства, и получаете доступ, делает возможным взлом за несколько часов с помощью перебора всего лишь 11000 вариантов.

Что делаем в целом

Новости на портале

Что ждет сотрудников, клюнувших на фишинг?!

09.08.2020 359 3 0

Киберпреступники лишат вас денег, работы и даже личной жизни практически в один клик мышки. Если вы им поможете. В июле компания провела тестовую рассылку фишинговых писем, и на крючок попалась почти тысяча сотр

Многие из вас помнят вирус Петя (Petya), программу-вымогатель, заразившую в 2017 году компьютеры компаний по всему миру этого года жертвой шифровальщика Рюк (Ryuk) стали наши американские коллеги: кибератака остановила производство на заводе назад хакеры парализовали работу крупного производителя систем навигации самолетов и фитнес-браслетов «Гармин» (Gar

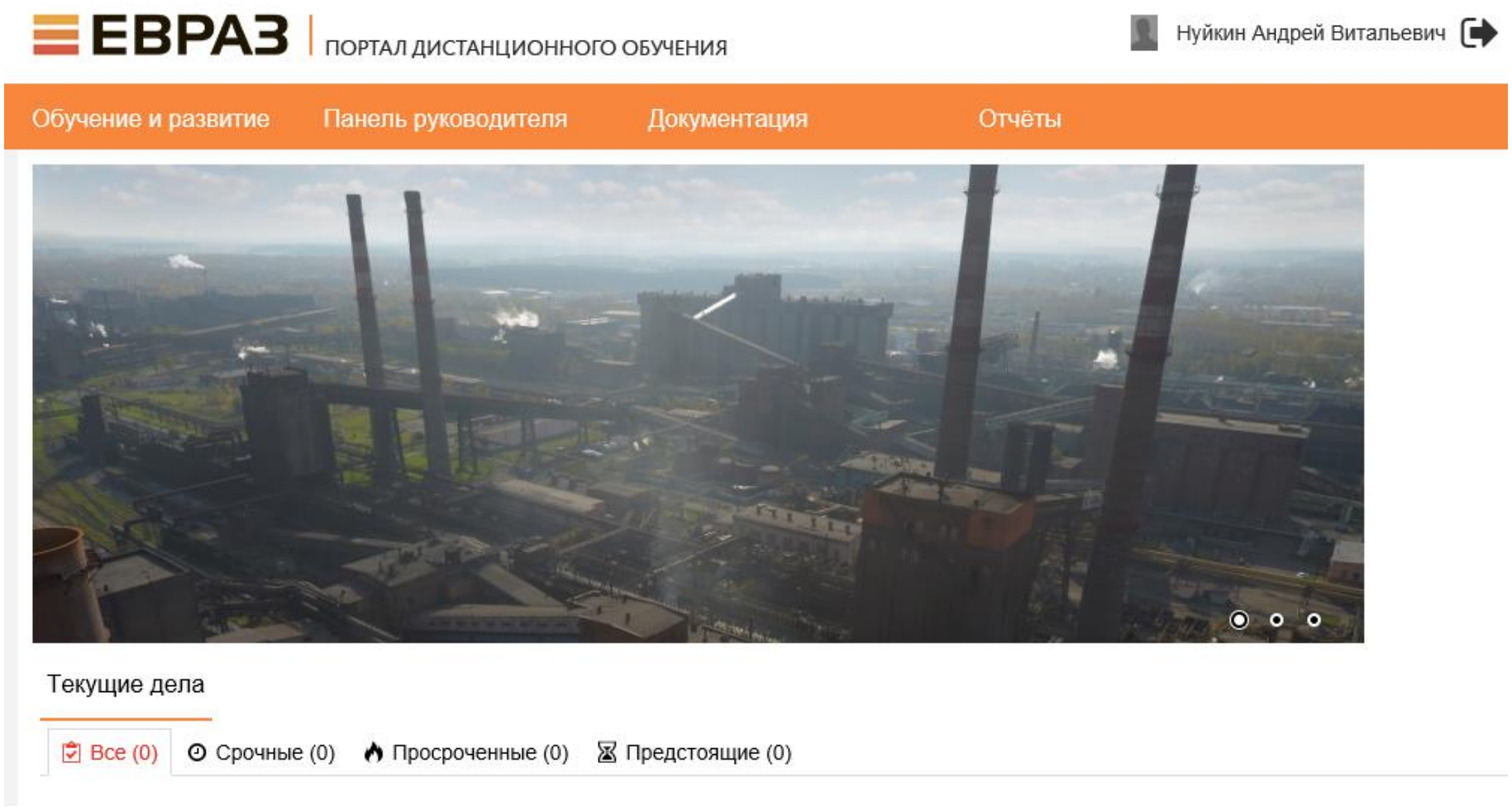
Внимание! Зафиксирован рост числа фишинговых сообщений

09.06.2020 662 5 0

Проследние дни специалисты Блока по ИТ фиксируют значительный рост числа фишинговых сообщений. Активность мошенников в сети возрасла. Пожалуйста, будьте внимательны при работе с электронной почтой.

Что делаем в целом

Система WebTutor



Определение цели

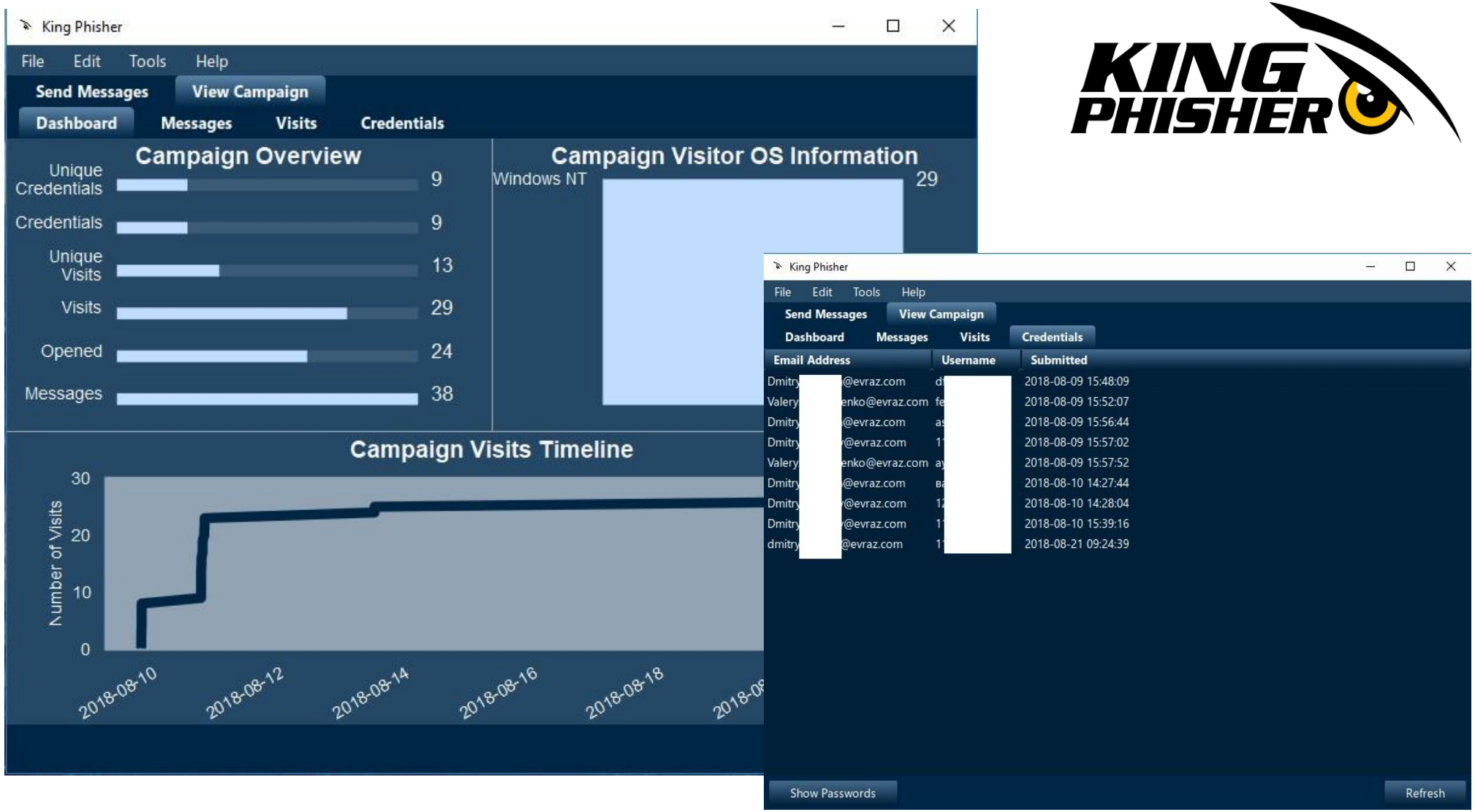
ЕВРАЗ

Цель:

1. Оценить вероятность утечки учетных данных от корпоративных учетных записей.
2. Повысить степень вовлеченности пользователей в процесс противодействия фишинговым атакам.
3. Повысить уровень осведомленности пользователей.
4. Оценить результаты мероприятий по обучению.

Подготовка

ЕВРАЗ



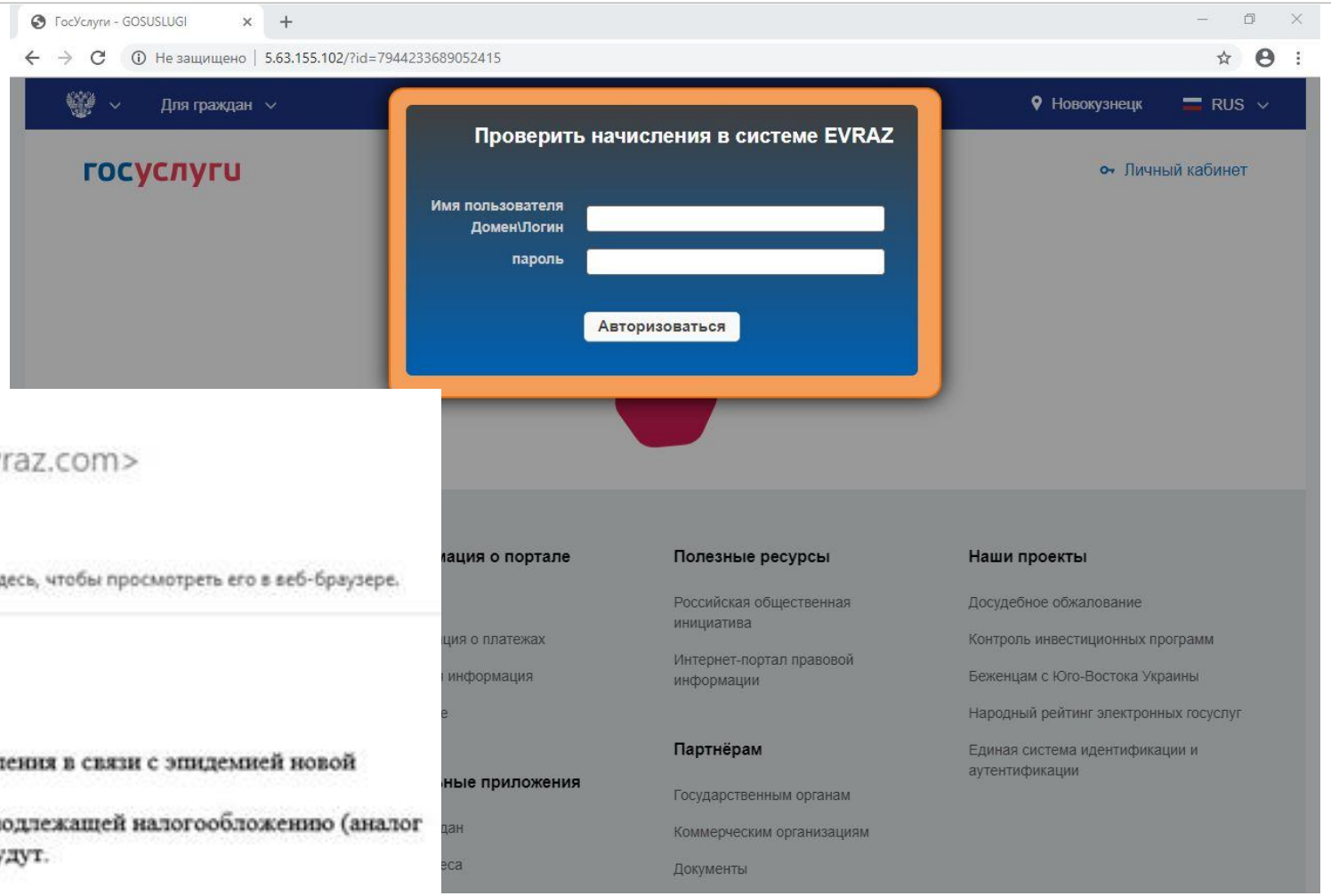
Масштабы охвата

Рассылка осуществлялась сотрудникам ООО «ЕвразХолдинг», управляемых предприятий Москвы, Урала, Сибири, Южных регионов России за исключением ТОП менеджеров.

За июль 2020 г. отправлено 16232 письма на 2 темы: «Госуслуги» (15725 писем) и «Прививки» (507 писем).

Тема «Госуслуги»

ЕВРАЗ




Пт 26.06.2020 16:55

"Дирекция" <econom.finanse@evraz.com>

Увеличение необлагаемой базы

Кому [redacted]

При наличии проблем с отображением этого сообщения щелкните здесь, чтобы просмотреть его в веб-браузере.

Добрый день!

Согласно указу Президента РФ «О мерах поддержки населения в связи с эпидемией новой коронавирусной инфекцией» от 23.06.2020 г.
Предлагаем заполнить заявление на увеличение базы, не подлежащей налогообложению (аналог налоговых вычетов). Суммы небольшие но лишними не будут.

С Уважением,
Служба по финансам и экономике

Тема «Прививки»

ЕВРАЗ

Пт 19.06.2020 16:13

"Охрана труда" <med.sanchast@evraz.com>

Планирование прививок от COVID

Кому [redacted]

При наличии проблем с отображением этого сообщения щелкните здесь, чтобы просмотреть его в веб-браузере.

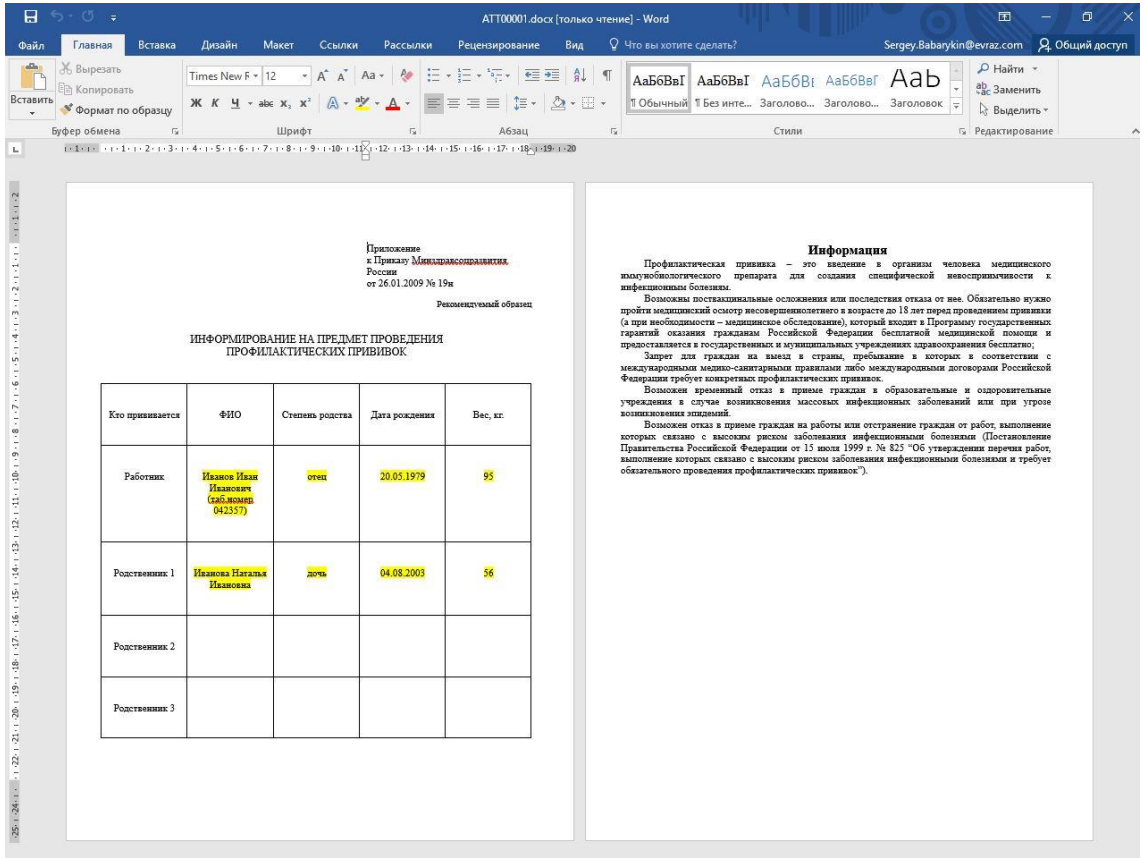
ATT00001.docx
22 KB

Важная информация!

Соглсно постановлению Правительства РФ от 03.04.2020 г. №434 угольная отрасль и металлургия входит в число пострадавших в условиях ухудшения ситуации в результате распространения новой коронавирусной инфекции.
Граждане, работающие в пострадавших отраслях, имеют право на воспользоваться как специально предусмотренными для таких отраслей мерами, так и общей для всего населения помощью.

Всем желающим необходимо заполнить заявление (по образцу, выделено желтым цветом) на бесплатные прививки от COVID-2-2019, помимо себя можно указать троих ближайших родственников. Списки и бюджет формируем сейчас, не затягивайте с предоставлением информации, прививки будут делаться БЕСПЛАТНО по мере разработки и поступления вакцины за счет средств работодателя. Заявление отправить по электронной почте
Ответить

С Уважением,
Медицинская служба



ЕВРАЗ

Количество откликов в Сервисдеск:

783 откликов на 16232 отправленных писем
или **4,8 откликов на 100 разосланных писем**

Результативность темы Госуслуги: $\frac{873\ \text{УЗ}}{15725\ \text{писем}} = 5{,}6\%$

5,6 скомпрометированных учетных записей на 100 писем

Результативность темы COVID-19: $\frac{105}{507\ \text{писем}} = 20{,}7\%$

20 скомпрометированных машин на 100 писем,
2 человека (0,4%) отправили файл с данными на стороннюю почту

Оценка поведения пользователей

ЕВРАЗ

Действия пользователей	Количество пользователей	%
Отреагировали	**783**	**4,8% к разосланным письмам**
из них сообщили в СД	741	94,6% к числу сообщивших
сообщили, но попались	42	5,4% к числу сообщивших
Попались и не сообщили	**873**	**5,4% к разосланным письмам**
из них, попались повторно	43	4,9% к числу попавшихся и не сообщивших
Ввели ложные данные	**31**	**0,2% к разосланным письмам**
Разослано писем ВСЕГО	**16232**	

Оценка поведения пользователей

Сравнение кампаний: июнь 2020 с декабрем 2019

ЕВРАЗ

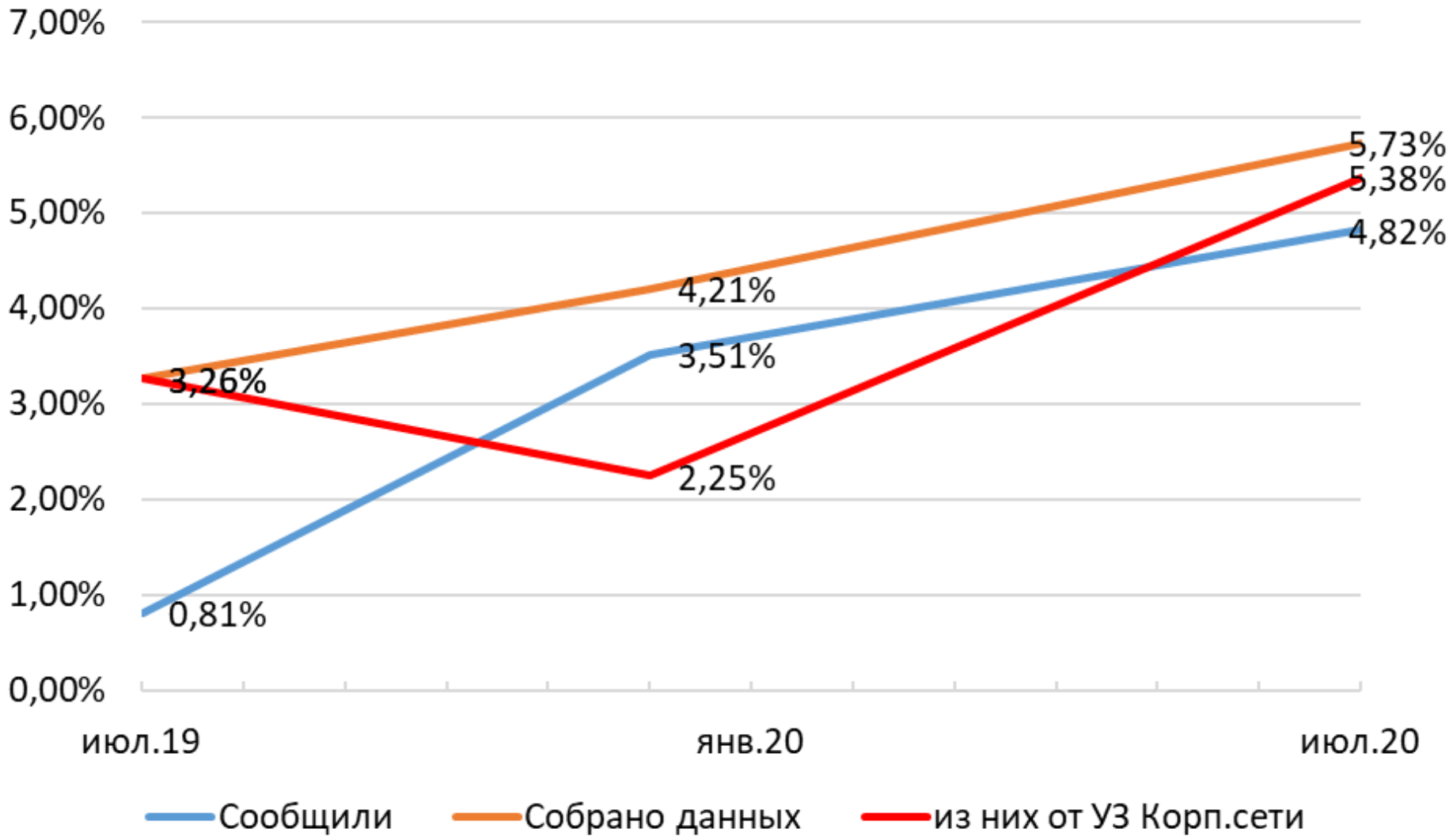
Результаты сравнения приведены в таблице

Наименование	июл.20		дек.19		Изменение, %
	Количество	% от отправленных	Количество	% от отправленных	
Отправлено	16232		15715		
Сообщили	783	4,82%	552	3,51%	1,31%
Собрано данных	930	5,73%	661	4,21%	1,52%
из них от УЗ Корп.сети	873	5,38%	353	2,25%	3,13%

Количество:

- сообщивших в техподдержку увеличилось на 1,3%
- оставивших данные от корпоративной сети увеличилось на 3,13%

Сравнение кампаний: динамика за 2019 – 2020 гг.



Итоги

ЕВРАЗ

Цель, связанная с повышением вовлеченности пользователей в процесс противодействия фишинговым атакам достигнута.

Выводы:

1. Вероятность утечки логинов и паролей от корпоративных учетных записей 5,3%, для ее реализации требуется разослать большое количество писем.
2. После начала рассылок первые заявки СД начинали приходить через 15 – 20 минут, при быстрой реакции со стороны ИТ-подразделений есть все шансы на своевременную блокировку e-mail злоумышленников и их web-ресурсов.
3. Пользователи чувствительны к теме рассылки. Если тема актуальна, то эффективность фишинга значительно возрастает – этим можно объяснить рост количества попавшихся на 3,13%.
4. Работу по повышению уровня осведомленности пользователей необходимо продолжать. По итогам рассылки будут скорректированы обучающие материалы, продолжена работа по периодическому информированию пользователей о тенденциях в области ИБ.

ЕВРАЗ

Спасибо за внимание

+7(495) 363-19-60

Andrey.nuykin@evraz.com

www.evraz.com