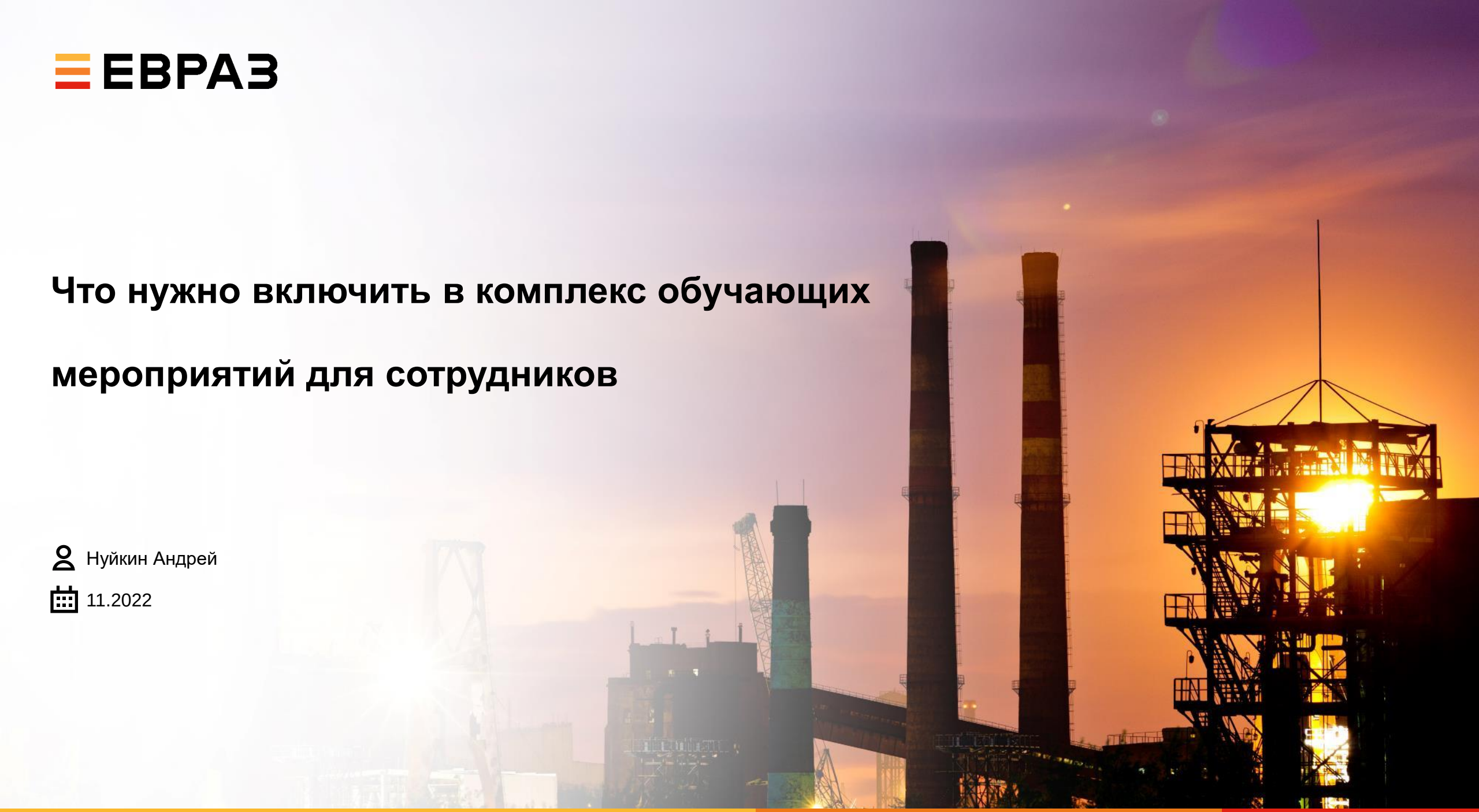
ЕВРАЗ

Что нужно включить в комплекс обучающих мероприятий для сотрудников



Нуйкин Андрей

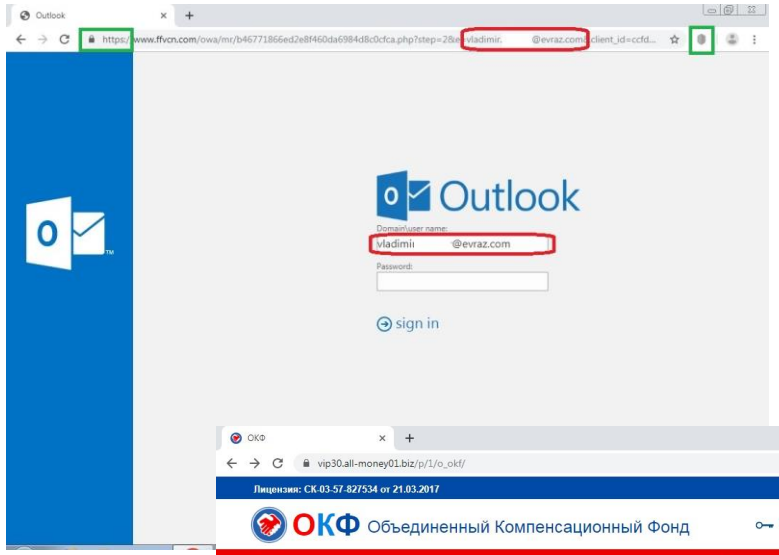
11.2022

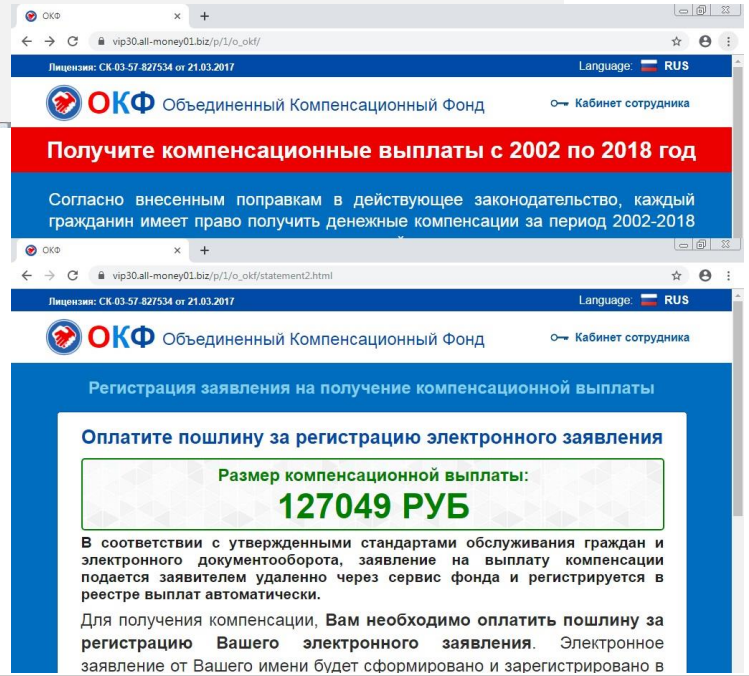
ЕВРАЗ

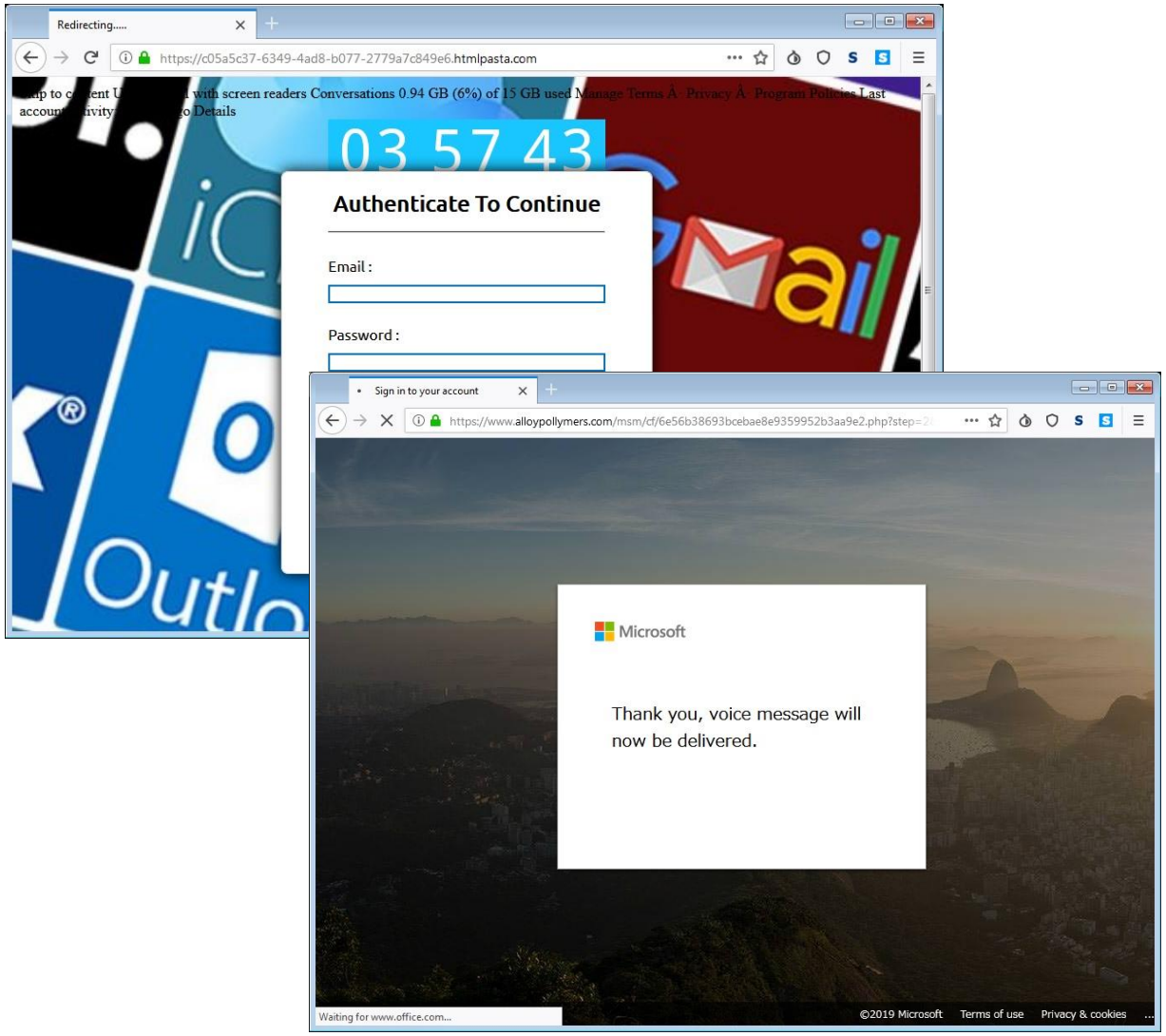
ЕВРАЗ является вертикально-интегрированной металлургической и горнодобывающей компанией с активами в России, США, Канаде и Казахстане. Компания входит в число крупнейших производителей стали в мире. Собственная база железной руды и коксующегося угля практически полностью обеспечивает внутренние потребности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

Текущая реальность

ЕВРАЗ







Текущая реальность

ЕВРАЗ

По данным Group-IB, ежедневно жертвами только финансового фишинга в России становятся свыше 900 клиентов различных банков, — этот показатель в 3 раза превышает ежедневное количество жертв от вредоносных программ. Ущерб от одной фишинговой атаки на пользователя варьируется от 2000 до 50 000 рублей. Мошенники не просто копируют сайт компании или банка, их логотипы и фирменные цвета, контент, контактные данные, регистрируют похожее доменное имя, они еще активно рекламируют свои ресурсы в соцсетях и поисковиках.

GROUP IB

positive technologies

По нашим оценкам, фишинг по-прежнему остается одним из главных методов атак, используемых злоумышленниками. Количество атак на частных лиц с использованием методов социальной инженерии заметно увеличилось: если в III квартале 2020 года доля таких атак составляла 67%, то за тот же квартал 2021 года она выросла до 83%. Злоумышленники не стоят на месте и постоянно совершенствуют методы обмана жертв. Объемы атак растут, а последствия наносят все больший ущерб. Фишинг считается второй по значимости причиной утечки данных

Текущая реальность

ЕВРАЗ

Microsoft

Пути заражения компьютера вредоносными программами

Security, Windows

Ниже приведены наиболее распространенные случаи заражения устройств вредоносными программами.

Письма со спамом

Авторы вредоносных программ часто пытаются обманным умыслом скачать вредоносные файлы. Это может быть письмо с вложенным файлом, который описывается как уведомление о доставке, возврат налогового платежа или счет по купленному билету. В письме может быть сказано, что необходимо открыть вложение, чтобы получить отправление или деньги.

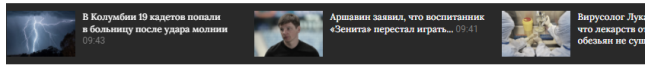
kaspersky

Компьютерные вирусы и вредоносное ПО: факты и часто задаваемые вопросы

Стандартные методы заражения

Итак, как же происходит заражение компьютерными вирусами или вредоносными программами? Существует несколько стандартных способов. Это ссылки на вредоносные сайты в электронной почте или сообщениях в социальных сетях, посещение зараженного сайта (известного как drive-by загрузка) и использование зараженного USB-накопителя на вашем компьютере. Уязвимости операционной системы и приложений позволяют злоумышленникам устанавливать вредоносное ПО на компьютеры. Поэтому для снижения риска заражения обновления для систем безопасности, как только они ста

газета.ru



03 декабря 2021, 14:03

В 2021 году почти половина россиян столкнулась с фишингом

Дони Джабборов

Прослушать новость

СПЕЦИАЛЬНЫЙ ПРОЕКТ RG.RU DIGITAL

SecurityLab.ru
by Positive Technologies

Фанаты Adidas пострадали от фишинга

20 июня, 2018

Пользователи всегда попадают на самые свежие мошеннические фишинг-атаки, хакеры используют эту слабость и скрывают свои интриги за обычными поддельными призами, которые оказываются слишком хорошими, чтобы быть настоящими подарками. На этот раз это была атака, использующая Adidas и нацеленная на пользователей в конкретных регионах.
Поддельная кампания Adidas обещала бесплатные ботинки. Для атаки хакеры использовали WhatsApp, такая схема в первый раз так активно использовалась в этом году.

Иван Черноусов
Автор материала

ПОСЛЕДНИЕ ЗАПИСИ АВТОРА

На российский рынок выходит новый смартфон среднего ценового сегмента от realme

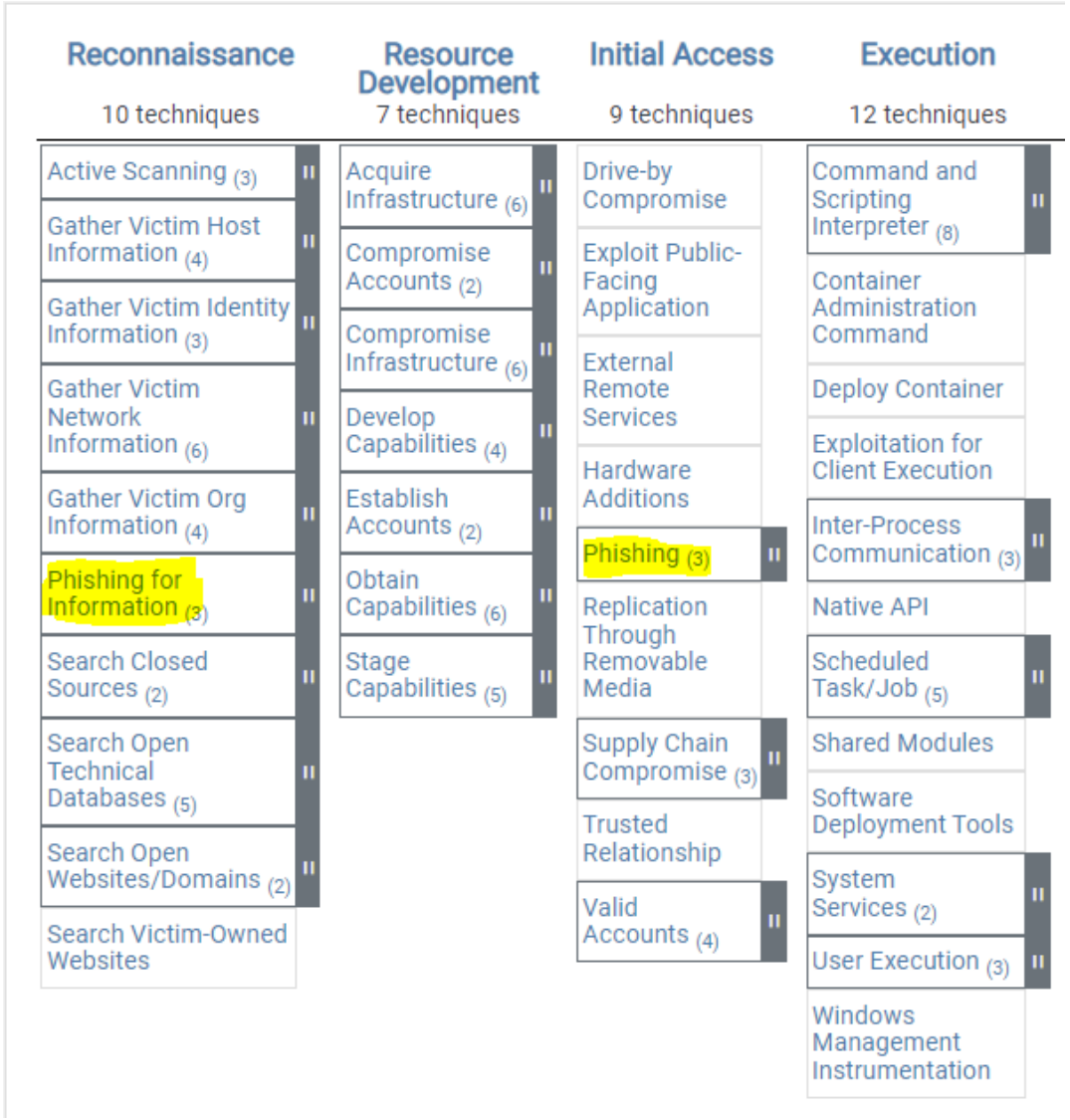
Большинство россиян готовы перейти в

Фишинговые атаки: как россияне стали жертвами онлайн-мошенников

Текст: Иван Черноусов 28.10.2020, 13:31

42% россиян сталкивались с фишингом, 27% стали его жертвами, и чуть больше трети (35%) не смогли дать точный ответ. При этом две трети респондентов, подвергшихся фишинговой атаке, пострадали, занимаясь личными вопросами, одна треть - решая рабочие задачи. Об этом сообщает компания Avast.

MITRE Att&ck Matrix



Reconnaissance	Resource Development	Initial Access	Execution
10 techniques	7 techniques	9 techniques	12 techniques
Active Scanning (3)	Acquire Infrastructure (6)	Drive-by Compromise	Command and Scripting Interpreter (8)
Gather Victim Host Information (4)	Compromise Accounts (2)	Exploit Public-Facing Application	Container Administration Command
Gather Victim Identity Information (3)	Compromise Infrastructure (6)	External Remote Services	Deploy Container
Gather Victim Network Information (6)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution
Gather Victim Org Information (4)	Establish Accounts (2)	Phishing (3)	Inter-Process Communication (3)
Phishing for Information (3)	Obtain Capabilities (6)	Replication Through Removable Media	Native API
Search Closed Sources (2)	Stage Capabilities (5)	Supply Chain Compromise (3)	Scheduled Task/Job (5)
Search Open Technical Databases (5)		Trusted Relationship	Shared Modules
Search Open Websites/Domains (2)		Valid Accounts (4)	Software Deployment Tools
Search Victim-Owned Websites			System Services (2)
			User Execution (3)
			Windows Management Instrumentation

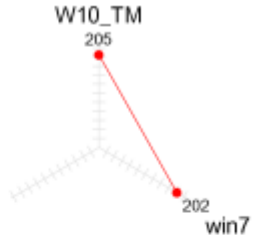
Что приходит в почте

ЕВРАЗ

Sources

Web	Email	Other Protocols	Endpoint	Manual
15	183	0	0	10

Infections by image



File types

HTML File	56
PDF 1.3	14
Office Word 2007 document	7
MS OLE document	6
ZIP archive	5
Excel 95 or 97 spreadsheet	4
Office Excel 2007 spreadsheet	2
General PDF	2

Malware types

Ransomware	7
Coin Miner	0
Web Threat	112
Dropper	95
Backdoor	79
Bot	13
Downloader	10
Worm	7
File infector	1
Others	1

ЕВРАЗ

В 2021-22 году количество атак программ-вымогателей на российские компании увеличилось более чем на 200%.

Каковы могут быть последствия

Средний размер требуемого выкупа вырос до 247 000 долларов США

РИА НОВОСТИ

09:39 14.05.2021 1898

Хакеры DarkSide похитили 740 гигабайт информации у Toshiba

ТОКИО, 14 мая – РИА Новости. Хакеры группировки DarkSide, которая, предположительно, совершила атаку на оператора трубопровода Colonial Pipeline в США, объявили о том, что похитили данные французского отделения японской корпорации Toshiba, соо
ссылкой на компанию по кибербезопасности M
Directions, Inc.

Как сообщила компания Mitsui Bussan Secure D
пятницу (19.00 мск четверга) хакерская группа
даркнете заявление, согласно которому она пс
секретной информации и персональных данны
японской корпорации Toshiba. Toshiba в свою
изучает этот вопрос.

RB.RU НОВОСТИ БИЗНЕС ТЕХНОЛОГИИ КАРЬЕРА РЕЛОКАЦИЯ ИМП

Атаковавшие Colonial Pipeline ха
использовали взломанный паро

НОВОСТИ 05 июня 2021

Виктория Сафронова
Редактор выходного дня RB.RU

Хакеры, причастные к кибератаке на систему трубопроводов компании Colonial Pipeline в США, воспользовались отсутствием многофакторной аутентификации на неиспользуемой учетной записи, пишет Bloomberg.

Инцидент был связан с неиспользующимся, но все еще активным входом в VPN, пишет Bloomberg.

По словам исполнительного директора Mandiant Чарльза Кармакала, анализ хакерской атаки показал, что подозрительная активность в сети Colonial Pipeline началась 29 апреля. Точного подтверждения способа, которым злоумышленники получили логин, пока нет, как и детальной информации о методах фишинга.

НОВОСТИ

Kaseya заявляет, что от вымогательской атаки пострадали около 1500 компаний

Мария Нефёдова , 06.07.2021 Комментарии 3,866

Пострадавшие компании получили записки с требованием выкупа в размере 50 000 долларов США (если зараженные машины не присоединены к домену) или 5 000 000 долларов США (если компьютер присоединен к домену, то есть является частью большой корпоративной сети).

Кроме того, операторы REvil потребовали выкуп в размере 70 миллионов долларов США, и тогда пообещали опубликовать универсальный дешифратор, который может разблокировать все компьютеры, пострадавшие после взлома Kaseya. В настоящее время хакеры "снизили планку" до 50 миллионов долларов.

Каковы могут быть последствия

ЕВРАЗ

Одно неосторожное открытие письма может привести
- к заражению компании вирусом
- к утечке конфиденциальных данных
- к технологическим сбоям, простоям и катастрофам на производстве

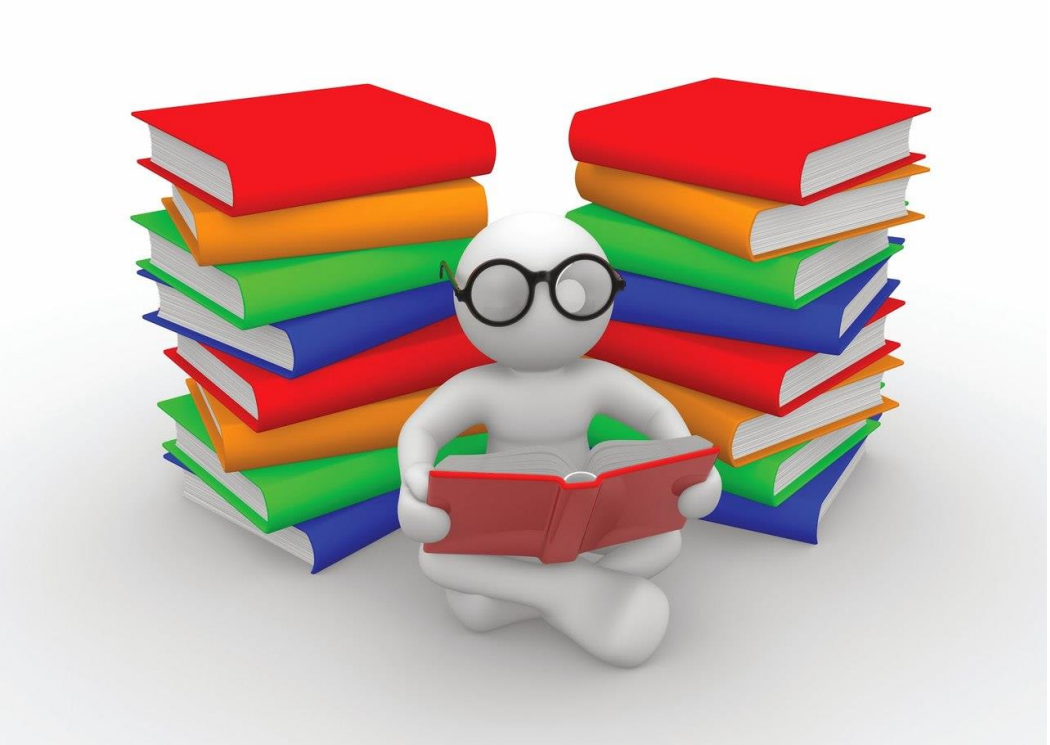
А это ведет к убыткам.

ЕВРАЗ

Пользователь слабое звено

ЕВРАЗ

Нужно постоянно обучать



Практика лучше теории

ЕВРАЗ

Можно купить комплексный продукт.

Стоимость зависит от модулей и количества пользователей.

Плюсы:

- Готовый продукт
- Полное сопровождение

Минусы:

- Стоимость

Можно сделать что-то свое.

Нужны специалисты по Linux и желание.

Плюсы:

- Низкая стоимость

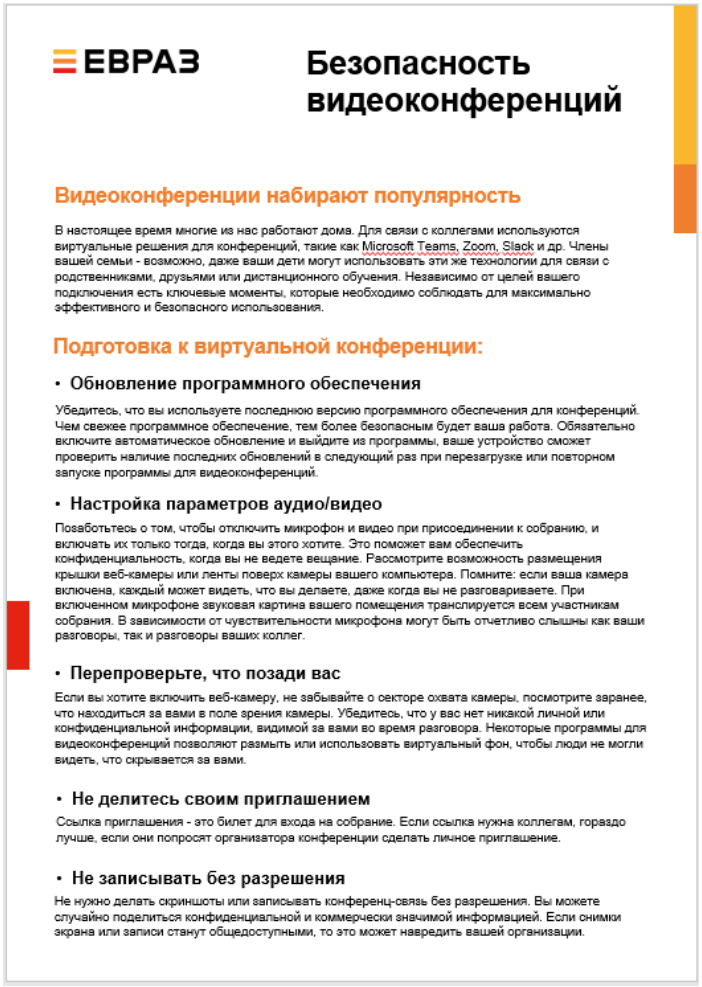
Минусы:

- Определенная сложность в установке
- Необходимо самостоятельно готовить все материалы

На самом деле все не так сложно

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**

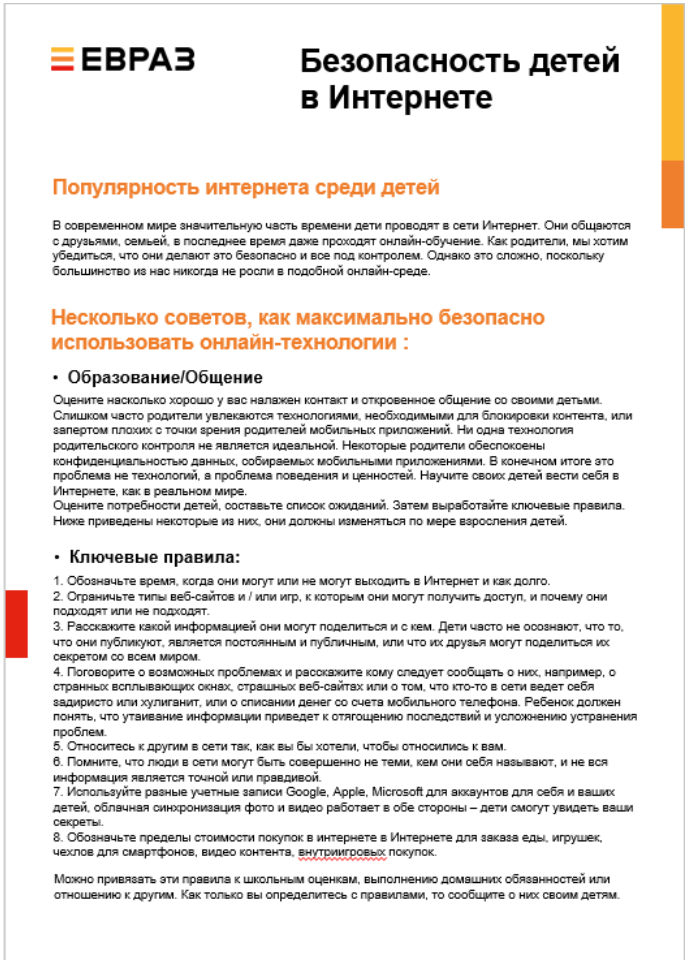
Если вы хотите включить веб-камеру, не забывайте о секторе охвата камеры, посмотрите заранее, что находиться за вами в поле зрения камеры. Убедитесь, что у вас нет никакой личной или конфиденциальной информации, видимой за вами во время разговора. Некоторые программы для видеоконференций позволяют размыть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

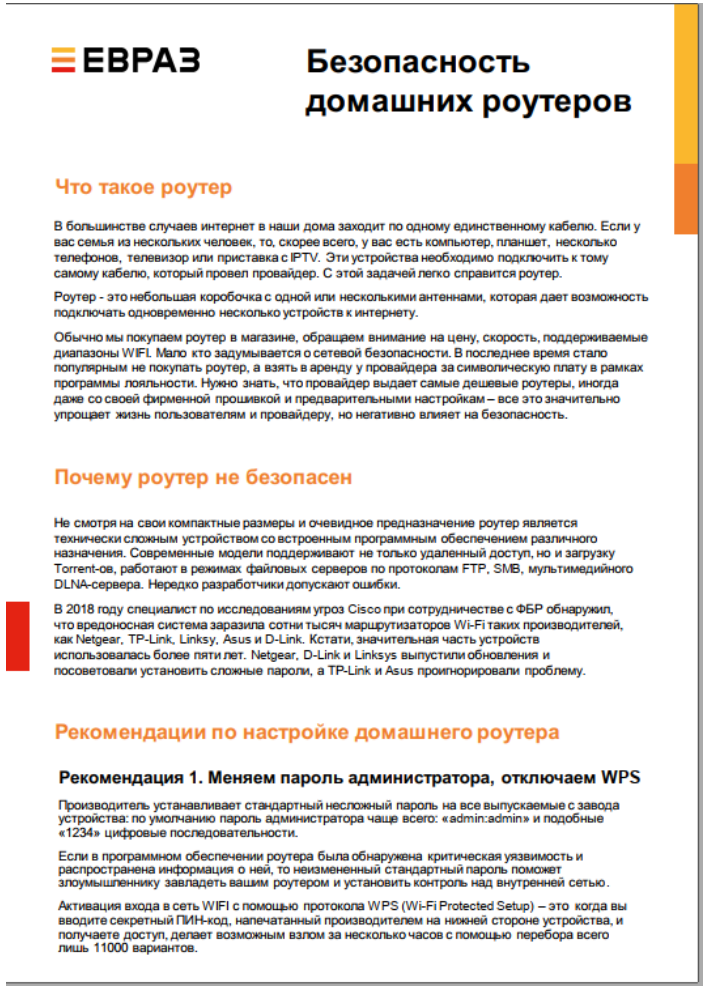
- **Образование/Общение**

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 сотрудников всех Дивизионов.

Многие из вас помнят вирус Петя (Petya), программу-вымогатель, заразившую в 2017 году компьютеры компаний по всему миру, в том числе ЕВРАЗа. В марте этого года жертвой шифровальщика Рюк (Ryuk) стали наши американские коллеги: кибератака остановила производство на заводах EVRAZ North America. Неделю назад хакеры парализовали работу крупного производителя систем навигации самолетов и фитнес-браслетов «Гармин» (Garmin). А вы все еще открываете

Внимание! Зафиксирована массовая рассылка фишинговых писем

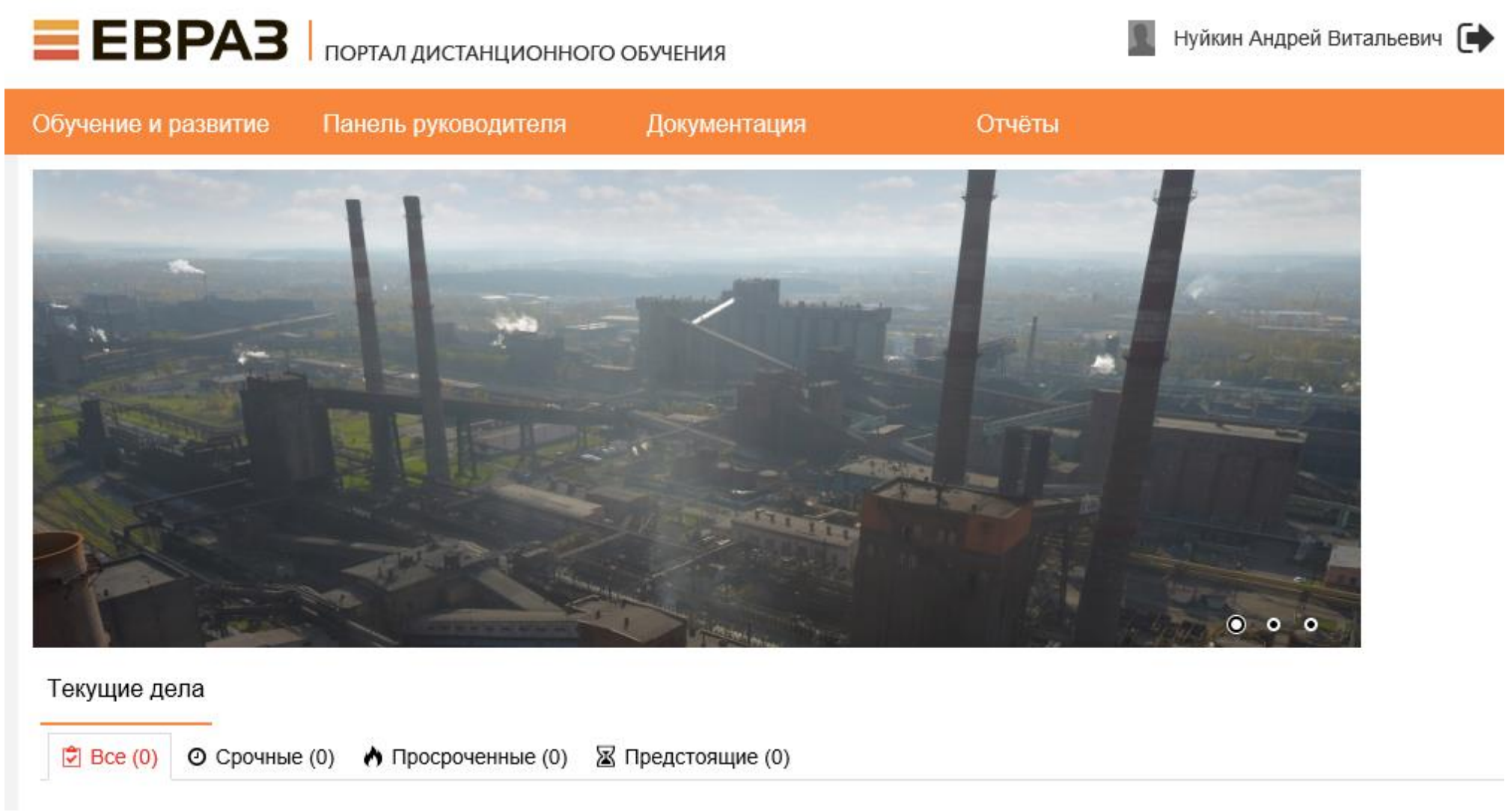
30.09.2021 12 1 1643

Сегодня наблюдается массовая рассылка фишинговых писем. В распространяемых сообщениях содержится вредоносный файл!

Уважаемые пользователи!

Сегодня наблюдается массовая рассылка фишинговых писем от имени государственных органов. В частности, зафиксированы сообщения от Федеральной Налоговой Службы.

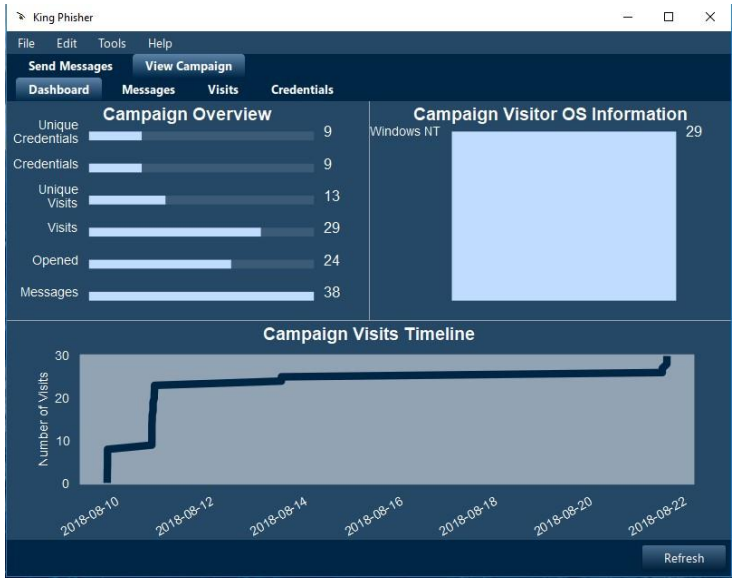
Что делаем в целом



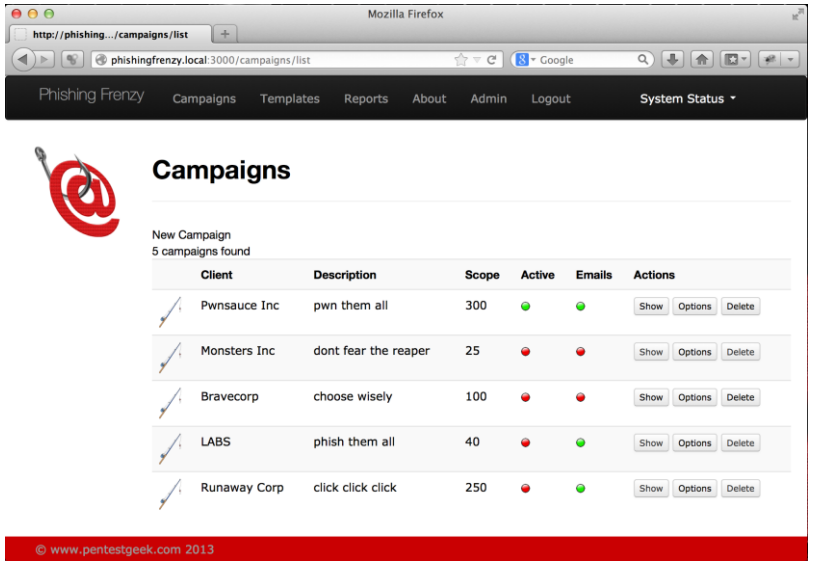
Как провести практическое обучение

ЕВРАЗ

KING PHISHER



PhishingFrenzy



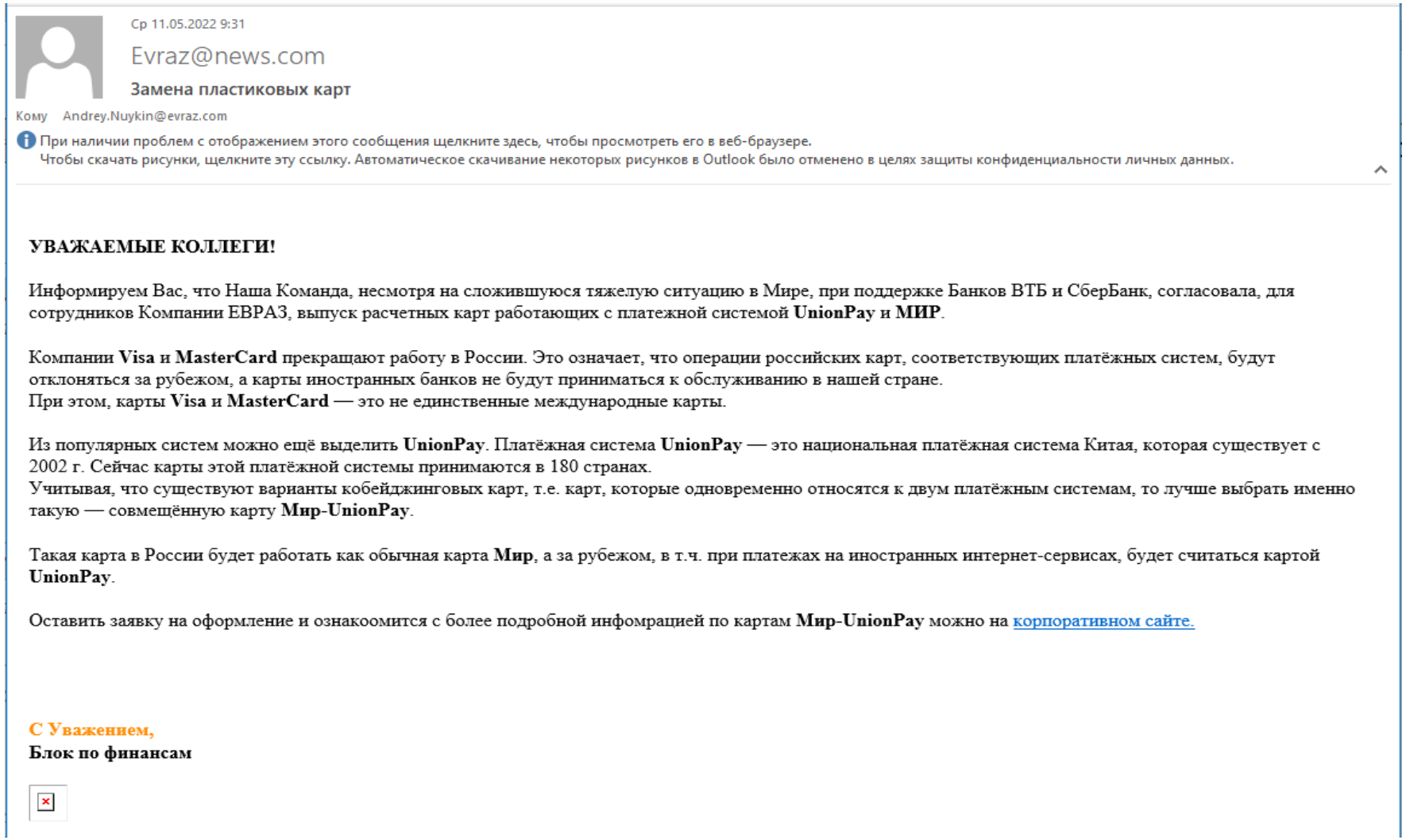
Масштабы охвата

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

Оценка поведения пользователей

Фишинговое письмо

Весной отправлялось письмо о замене зарплатных карт



Ср 11.05.2022 9:31

Evraz@news.com

Замена пластиковых карт

Кому Andrey.Nuykin@evraz.com

При наличии проблем с отображением этого сообщения щелкните здесь, чтобы просмотреть его в веб-браузере.
Чтобы скачать рисунки, щелкните эту ссылку. Автоматическое скачивание некоторых рисунков в Outlook было отменено в целях защиты конфиденциальности личных данных.

УВАЖАЕМЫЕ КОЛЛЕГИ!

Информируем Вас, что Наша Команда, несмотря на сложившуюся тяжелую ситуацию в Мире, при поддержке Банков ВТБ и СберБанк, согласовала, для сотрудников Компании ЕВРАЗ, выпуск расчетных карт работающих с платежной системой **UnionPay** и **МИР**.

Компании **Visa** и **MasterCard** прекращают работу в России. Это означает, что операции российских карт, соответствующих платёжных систем, будут отклоняться за рубежом, а карты иностранных банков не будут приниматься к обслуживанию в нашей стране.
При этом, карты **Visa** и **MasterCard** — это не единственные международные карты.

Из популярных систем можно ещё выделить **UnionPay**. Платёжная система **UnionPay** — это национальная платёжная система Китая, которая существует с 2002 г. Сейчас карты этой платёжной системы принимаются в 180 странах.
Учитывая, что существуют варианты кобейджинговых карт, т.е. карт, которые одновременно относятся к двум платёжным системам, то лучше выбрать именно такую — совмещённую карту **Мир-UnionPay**.

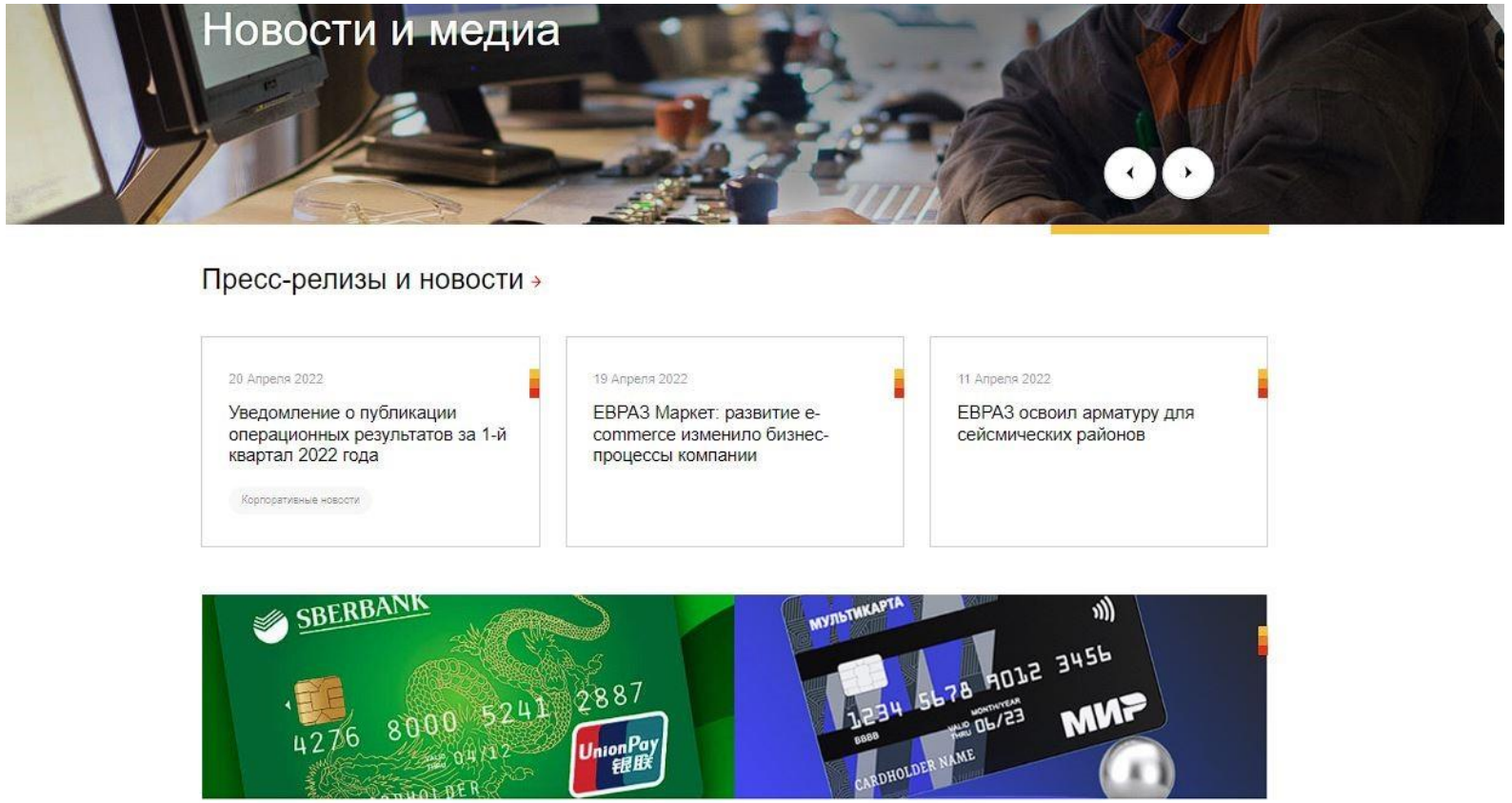
Такая карта в России будет работать как обычная карта **Мир**, а за рубежом, в т.ч. при платежах на иностранных интернет-сервисах, будет считаться картой **UnionPay**.

Оставить заявку на оформление и ознакоомится с более подробной инфомрацией по картам **Мир-UnionPay** можно на корпоративном сайте.

С Уважением,
Блок по финансам

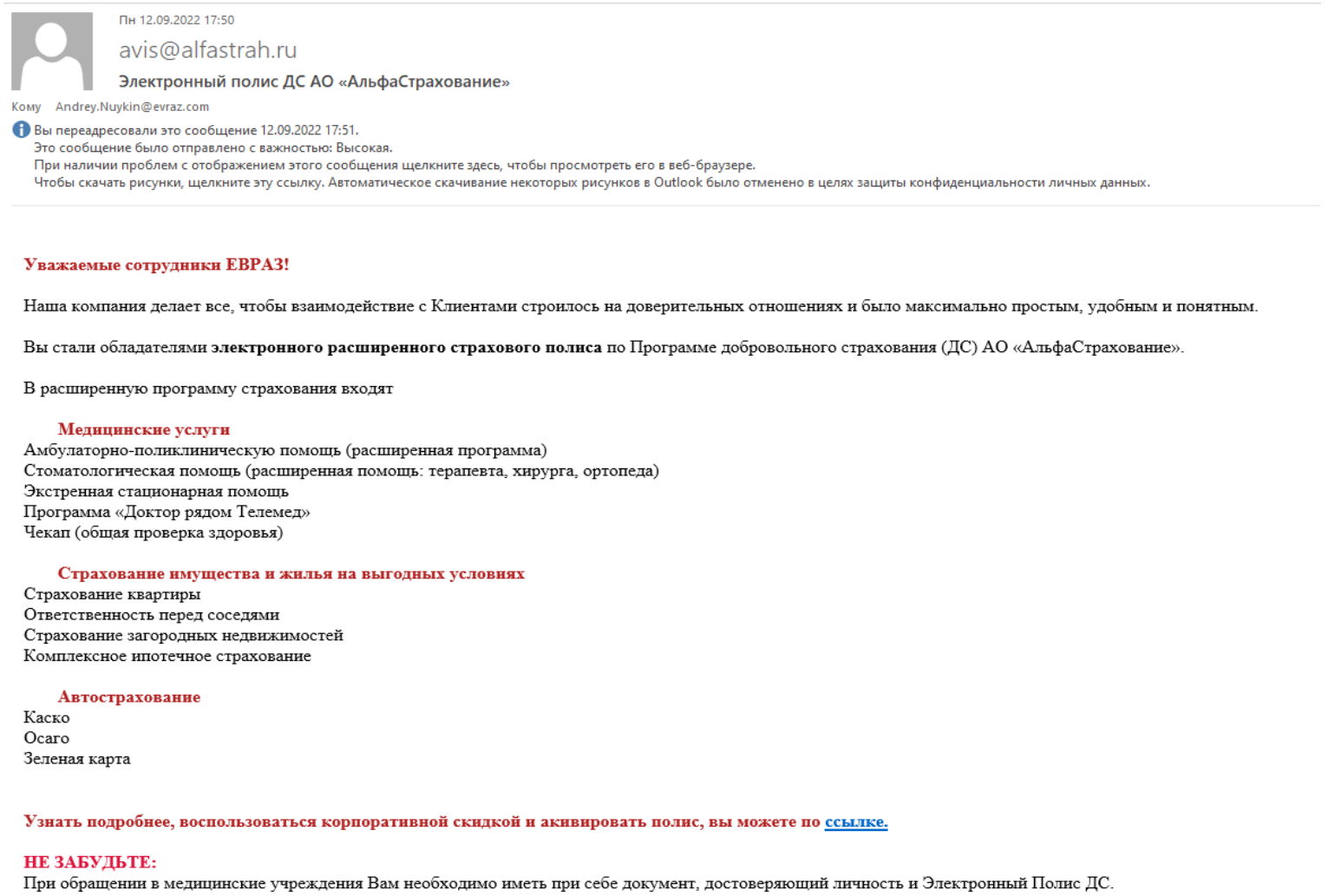
Фишинговое письмо

Фишинговая страница



Фишинговое письмо

Осенью отправлялось письмо от имени АльфаСтрахования.



Пн 12.09.2022 17:50

avis@alfastrah.ru

Электронный полис ДС АО «АльфаСтрахование»

Кому Andrey.Nuykin@evraz.com

Вы переадресовали это сообщение 12.09.2022 17:51.
Это сообщение было отправлено с важностью: Высокая.
При наличии проблем с отображением этого сообщения щелкните здесь, чтобы просмотреть его в веб-браузере.
Чтобы скачать рисунки, щелкните эту ссылку. Автоматическое скачивание некоторых рисунков в Outlook было отменено в целях защиты конфиденциальности личных данных.

Уважаемые сотрудники ЕВРАЗ!

Наша компания делает все, чтобы взаимодействие с Клиентами строилось на доверительных отношениях и было максимально простым, удобным и понятным.

Вы стали обладателями **электронного расширенного страхового полиса** по Программе добровольного страхования (ДС) АО «АльфаСтрахование».

В расширенную программу страхования входят

Медицинские услуги
Амбулаторно-поликлиническую помощь (расширенная программа)
Стоматологическая помощь (расширенная помощь: терапевта, хирурга, ортопеда)
Экстренная стационарная помощь
Программа «Доктор рядом Телемед»
Чекап (общая проверка здоровья)

Страхование имущества и жилья на выгодных условиях
Страхование квартиры
Ответственность перед соседями
Страхование загородных недвижимостей
Комплексное ипотечное страхование

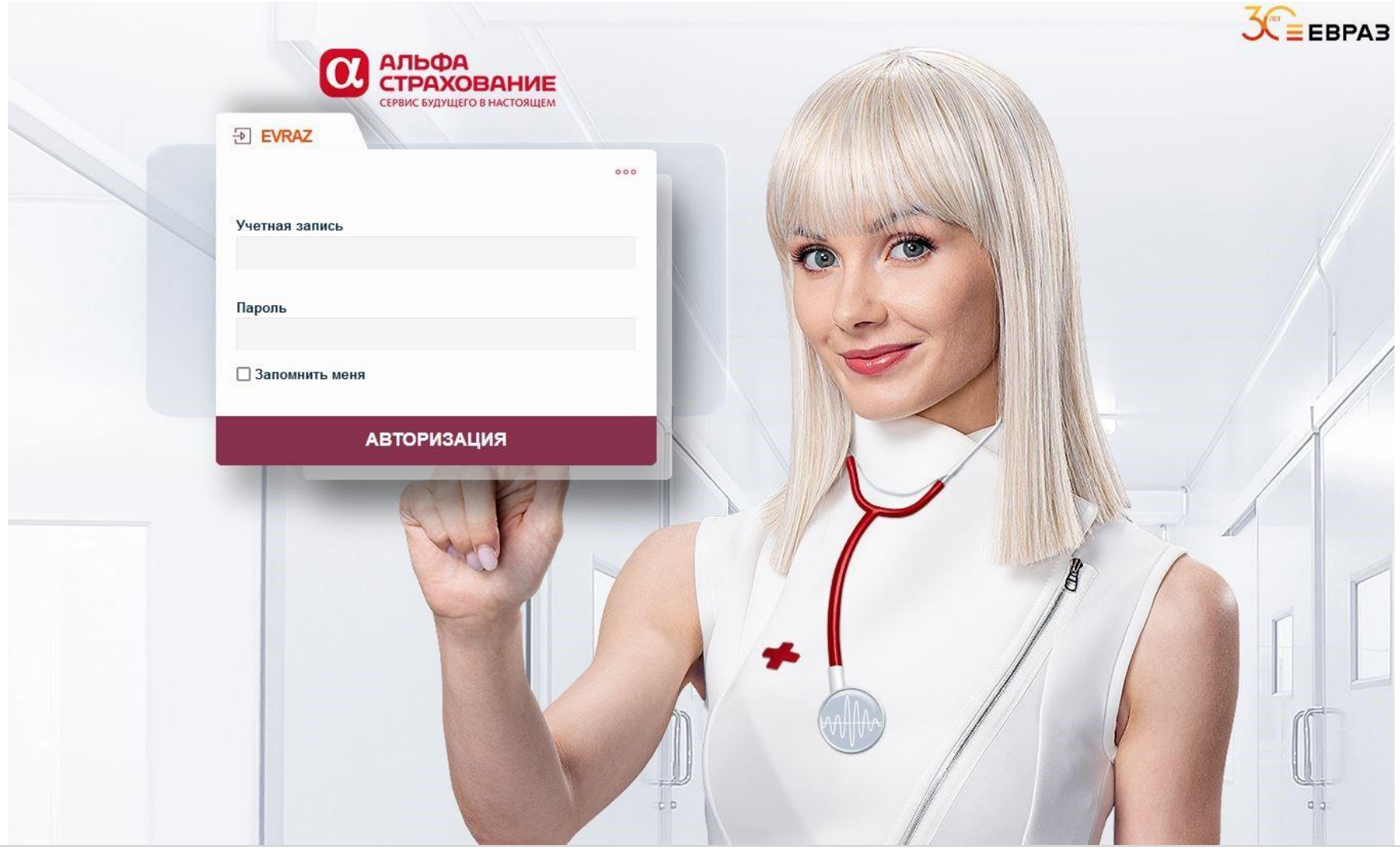
Автострахование
Каско
Осаго
Зеленая карта

Узнать подробнее, воспользоваться корпоративной скидкой и акивировать полис, вы можете по ссылке.

НЕ ЗАБУДЬТЕ:
При обращении в медицинские учреждения Вам необходимо иметь при себе документ, достоверяющий личность и Электронный Полис ДС.

Фишинговое письмо

Фишинговая страница



Результаты обучения

ЕВРАЗ

Весна

20 тыс. Писем отправлено	1692 Не доставленные письма	18 тыс. Доставленные письма
433 Заявки	1905 Посетили сайт	960 Пароли
2,38% Процент заявок	10,5% Процент посещения сайта	5,28% Процент паролей

Осень

20 тыс. Писем отправлено	1275 Не доставленные письма	19 тыс. Доставленные письма
274 Заявки	1066 Посетили сайт	691 Пароли
1,47% Процент заявок	5,7% Процент посещения сайта	3,71% Процент паролей

Как реагируют пользователи после обучения

ЕВРАЗ

За месяц около 200-400 обращений.

Описание

Предупреждение об атаке прошу проверить адрес FW: нужны данные

Информация

Прошу проверить адрес
[cid:image001.jpg@01D85FDB.006F99A0]

Описание

FW: Payment Copy!

Информация

Добрый день прошу проверить на спам и наличие вирусов

Описание

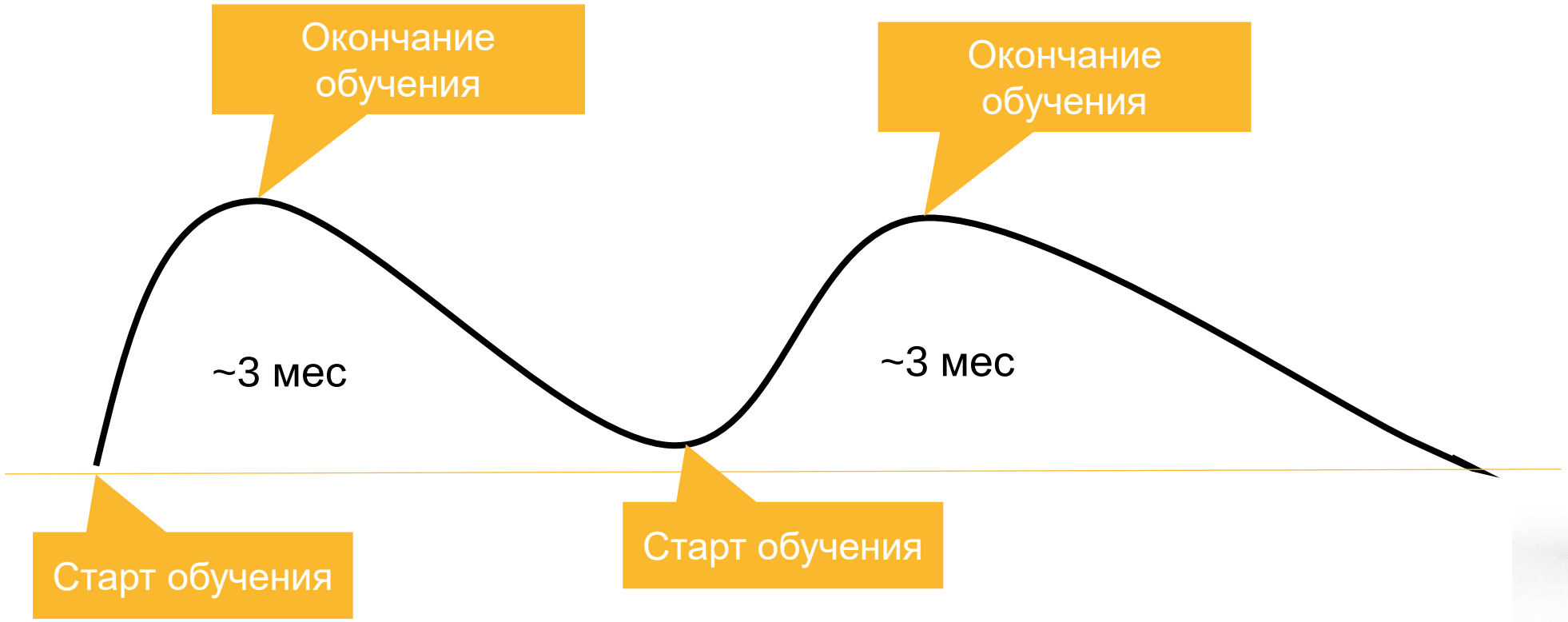
Плохое сообщение?

Информация

Коллеги, добрый день

Во вложении - сообщение мне со ссылкой, похоже на фишинг.

Как реагируют пользователи после обучения



Итоги

ЕВРАЗ

Количество фишинговых атак постоянно растет.

Достаточно одного открытого письма, чтобы скомпрометировать свою инфраструктуру.

Выводы:

1. Нужно постоянно работать с пользователями по повышению их осведомленности в области ИБ.
2. Нужно использовать различные каналы – новости, рассылки, курсы, практические учения
3. Добиться 100% защиты не получится, но нужно охватить максимально возможную аудиторию.

ЕВРАЗ

Спасибо за внимание

Андрей Нуйкин
CISA, CISM
АРСИБ
RuSCADASec Coin #29

+7(495) 363-19-60

Andrey.nuykin@evraz.com

www.evraz.com