ЕВРАЗ

Информационная безопасность: что нужно включить в комплекс обучающих мероприятий для сотрудников

Нуйкин Андрей

09.2024

О чем поговорим

ЕВРАЗ

Количество атак растет

Одним из основных векторов атаки являются сотрудники

От знаний сотрудников ИБ зависит благополучие компании

Время выступления – 15 минут

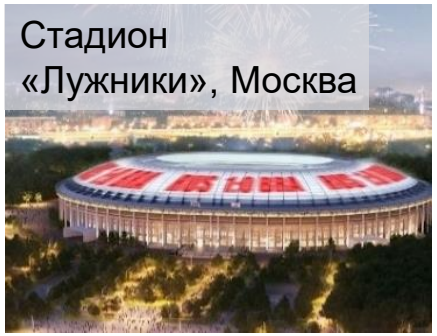
Вопросы после доклада – 5 минут

Что такое ЕВРАЗ?

ЕВРАЗ


Олимпийские объекты, Сочи


Лахта центр, Санкт-Петербург

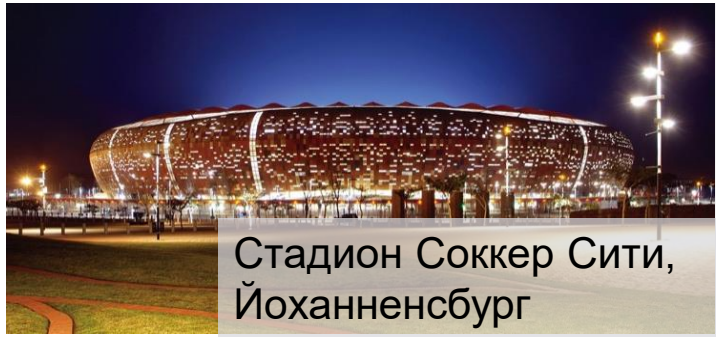

Стадион «Лужники», Москва


Амурский ГПЗ, Дальний Восток


Burj Al Arab Jumeirah, Дубай


Нефтегазовый комплекс Ямал СПГ


Спортивные объекты, Казань


Стадион Соккер Сити, Йоханненсбург


Красноярская ГЭС и Саяно-Шушенская ГЭС

Кто мы

ЕВРАЗ

- Три больших локации – Москва, Сибирь, Урал
- Порядка 150 проектов цифровизации в год
- Более 15 000 пользователей
- Порядка 3 000 000 писем в месяц
- В среднем 5 000 фишинговых писем
- Порядка 1000 вирусов и 18 000 подозрительных URL

Кто мы

ЕВРАЗ

- Более 20 лет в ИБ.
- Член АРСИБ, БИП-Клуба, КУБИТ.
- Работал в различных крупных компаниях: «Евроцемент», «Промсвязьбанк», SELA и др.
- С 2014 г. — начальник управления информационной безопасности в ЕВРАЗ.

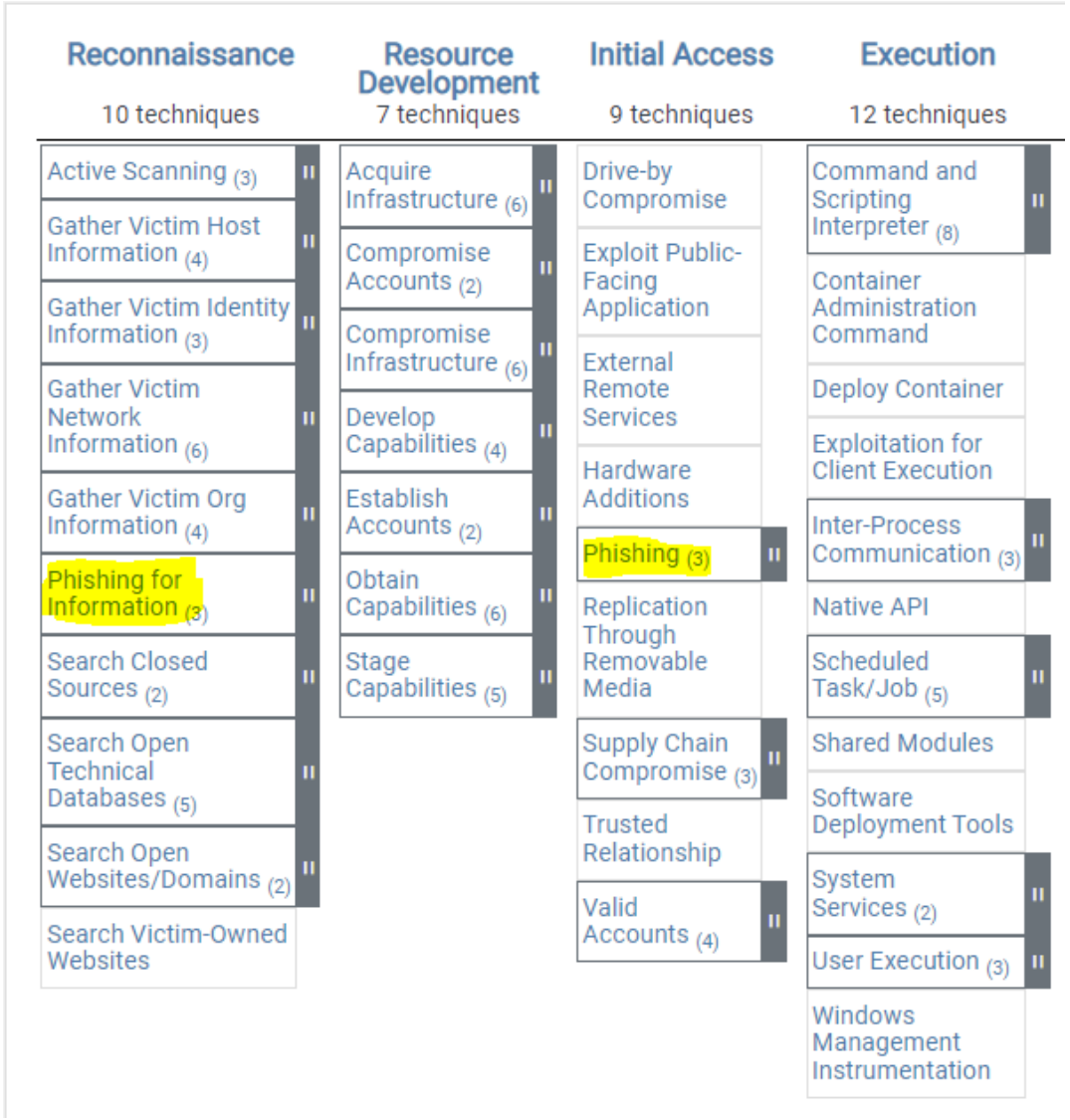
Андрей Нуйкин
CISA, CISM, CRISK
АРСИБ
RuSCADASec Coin #29

Что происходит?

ЕВРАЗ

В 2023-24 году количество атак на российские компании увеличилось более чем на 200%

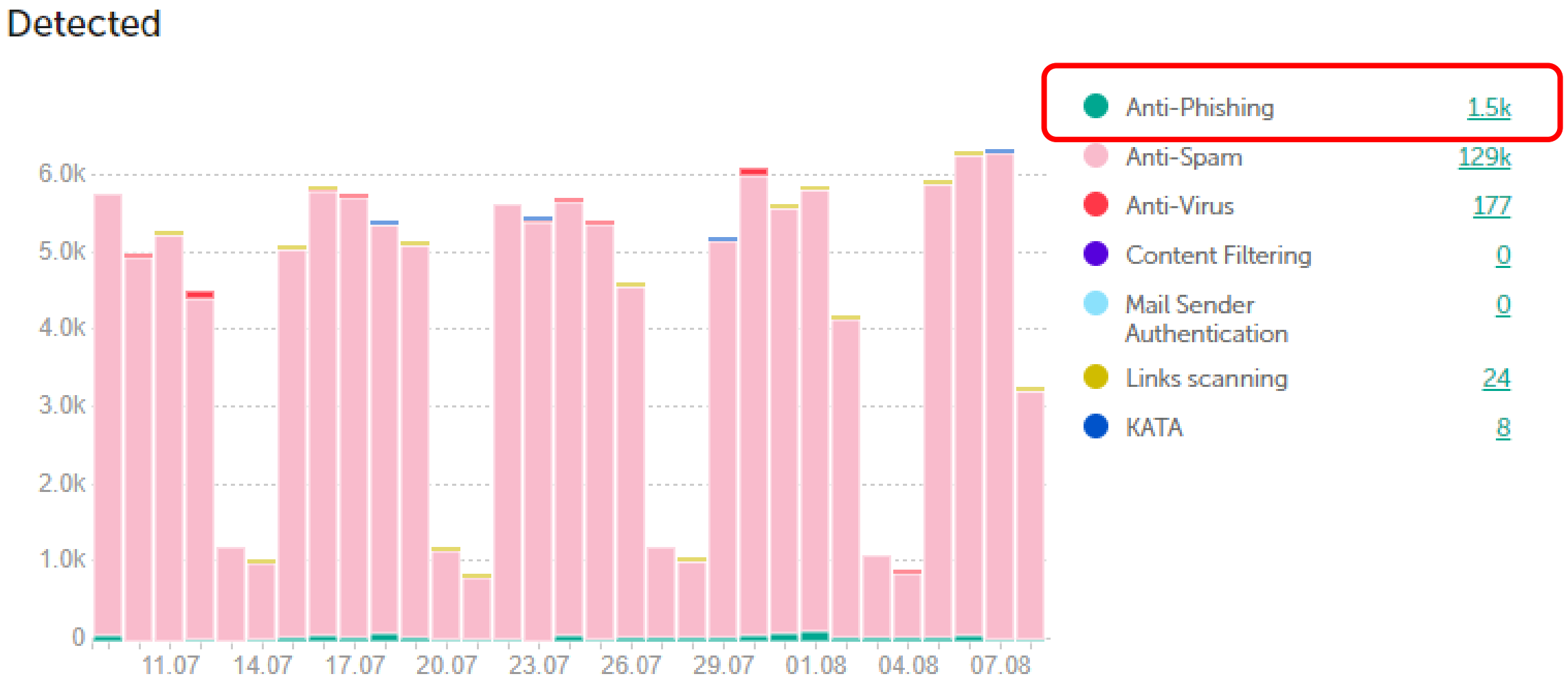
MITRE Att&ck Matrix



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

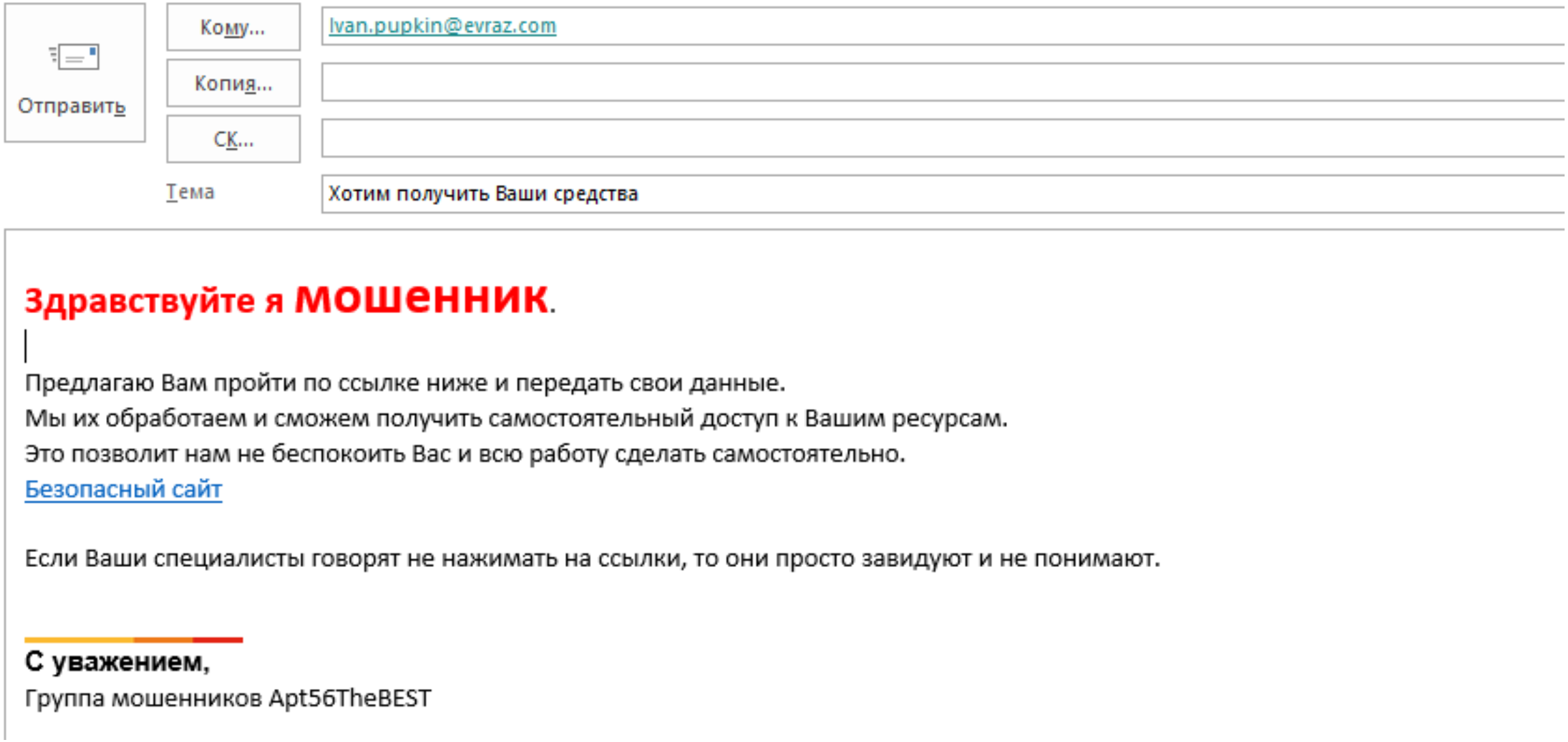


ЕВРАЗ

Пользователь слабое звено

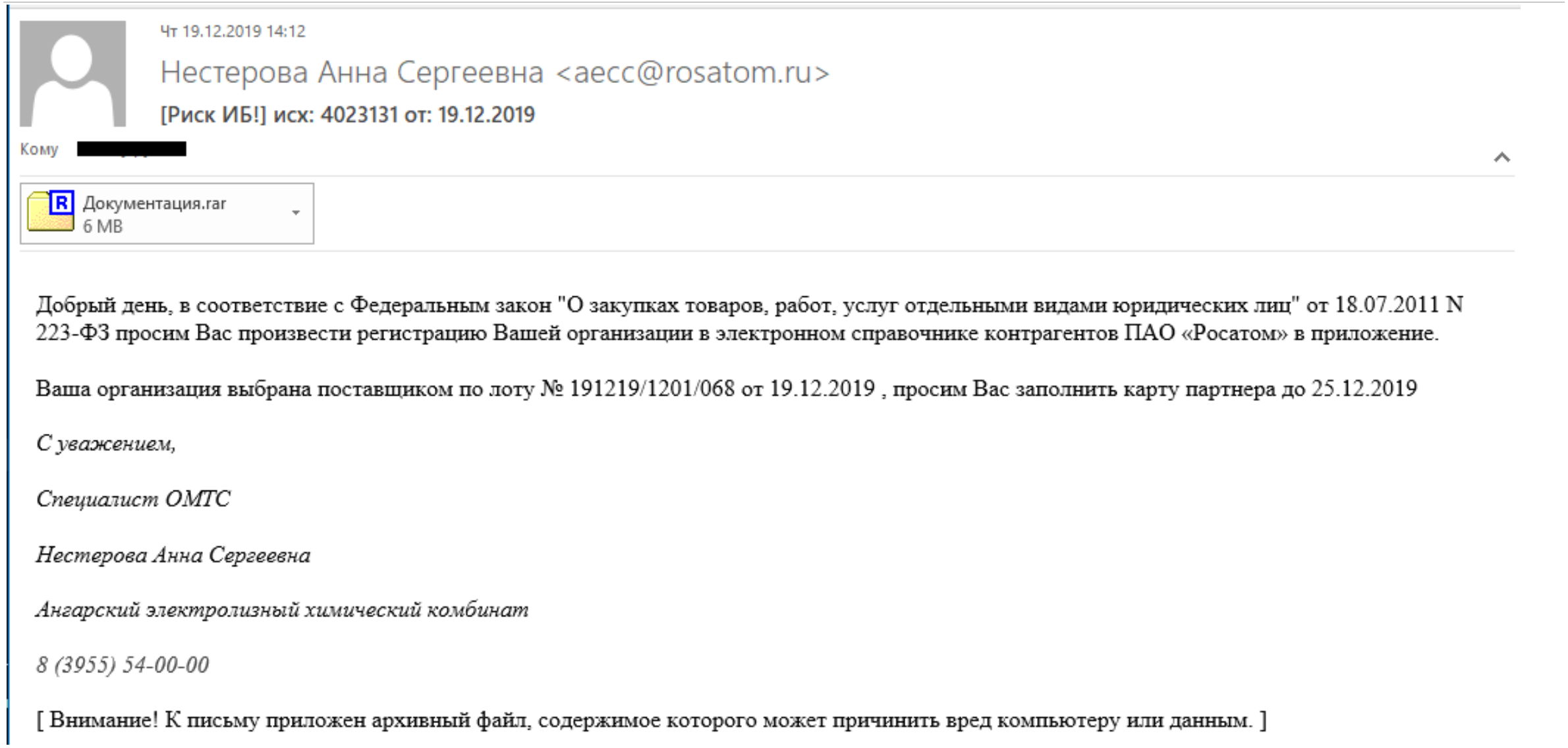
Как по мнению пользователей выглядит фишинговое письмо

ЕВРАЗ



Как на самом деле выглядит фишинговое письмо

ЕВРАЗ



Чт 19.12.2019 14:12

Нестерова Анна Сергеевна <aecc@rosatom.ru>

[Риск ИБ!] исх: 4023131 от: 19.12.2019

Кому [redacted]

Документация.rar
6 MB

Добрый день, в соответствие с Федеральным закон "О закупках товаров, работ, услуг отдельными видами юридических лиц" от 18.07.2011 N 223-ФЗ просим Вас произвести регистрацию Вашей организации в электронном справочнике контрагентов ПАО «Росатом» в приложение.

Ваша организация выбрана поставщиком по лоту № 191219/1201/068 от 19.12.2019 , просим Вас заполнить карту партнера до 25.12.2019

С уважением,

Специалист ОМТС

Нестерова Анна Сергеевна

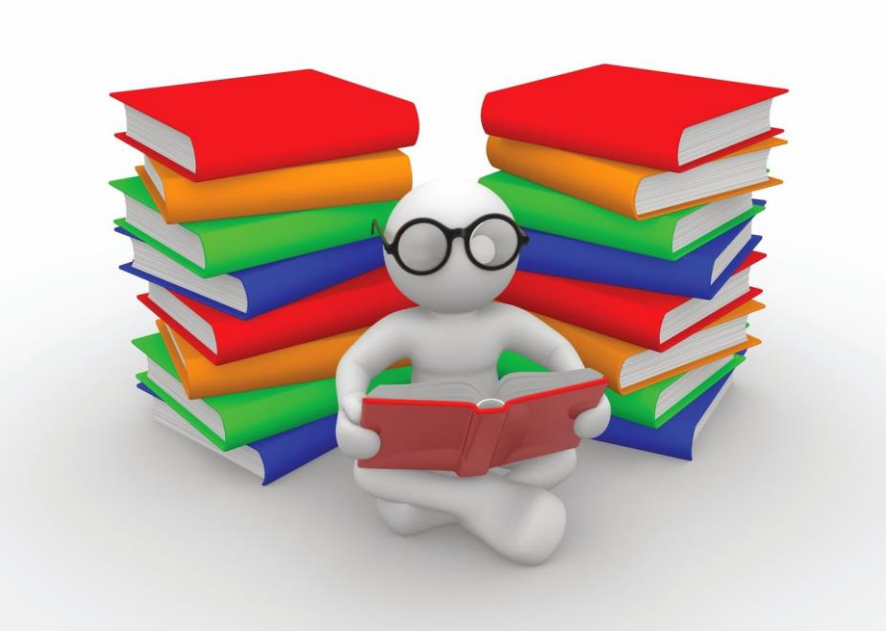
Ангарский электролизный химический комбинат

8 (3955) 54-00-00

[Внимание! К письму приложен архивный файл, содержимое которого может причинить вред компьютеру или данным.]

ЕВРАЗ

Нужно постоянно обучать



Практика лучше теории

Как организовать обучение?

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

Построим процесс повышения осведомленности без СМС и регистрации за минимальный бюджет

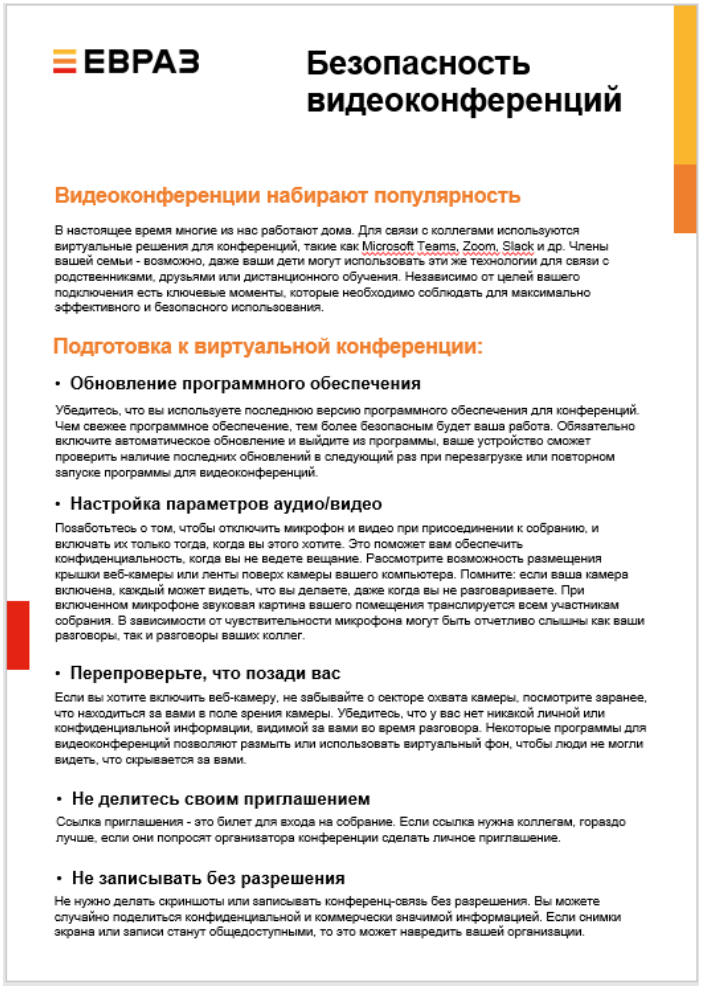
ЕВРАЗ

1. Рассказывать пользователям о правилах ИБ
2. Обучать пользователей по различным направлениям ИБ
3. Проводить практические занятия для закрепления навыков

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**

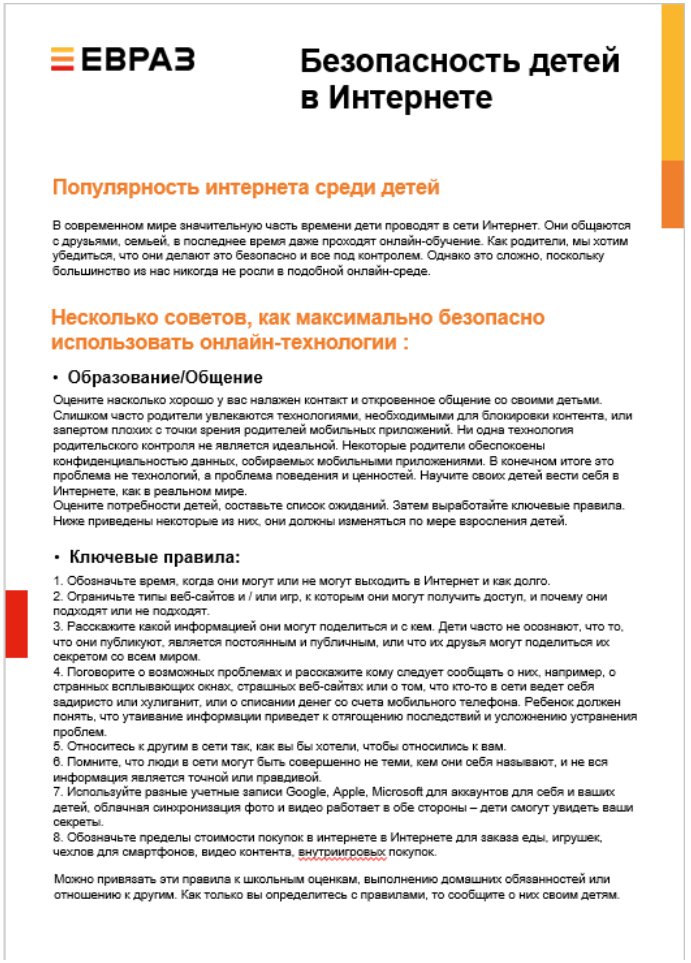
Если вы хотите включить веб-камеру, не забывайте о секторе охвата камеры, посмотрите заранее, что находиться за вами в поле зрения камеры. Убедитесь, что у вас нет никакой личной или конфиденциальной информации, видимой за вами во время разговора. Некоторые программы для видеоконференций позволяют размыть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

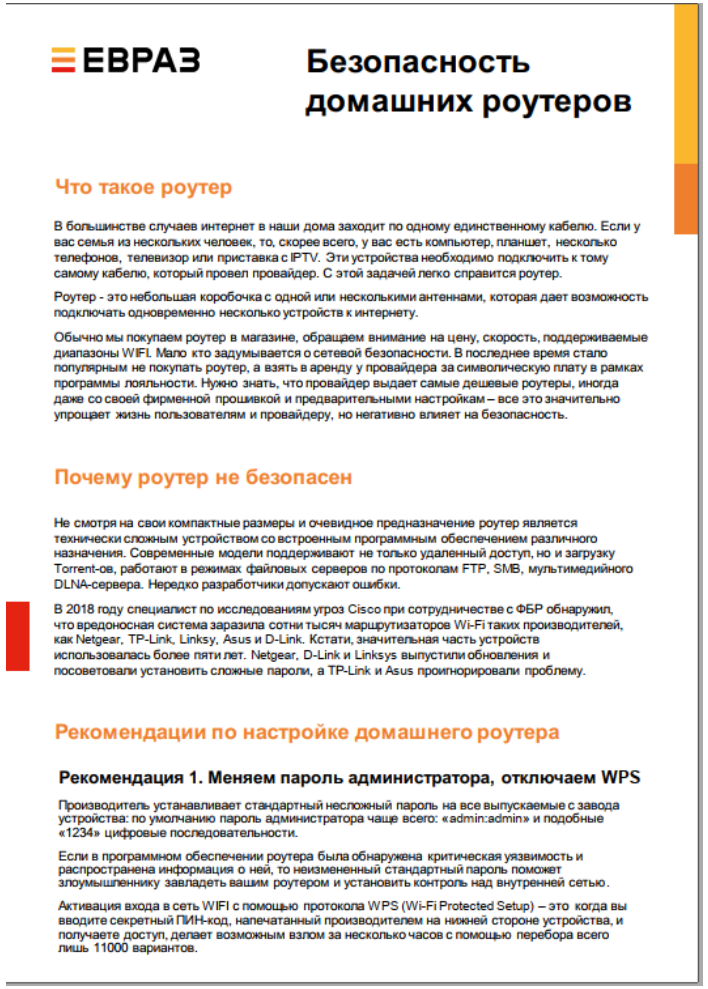
- **Образование/Общение**

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

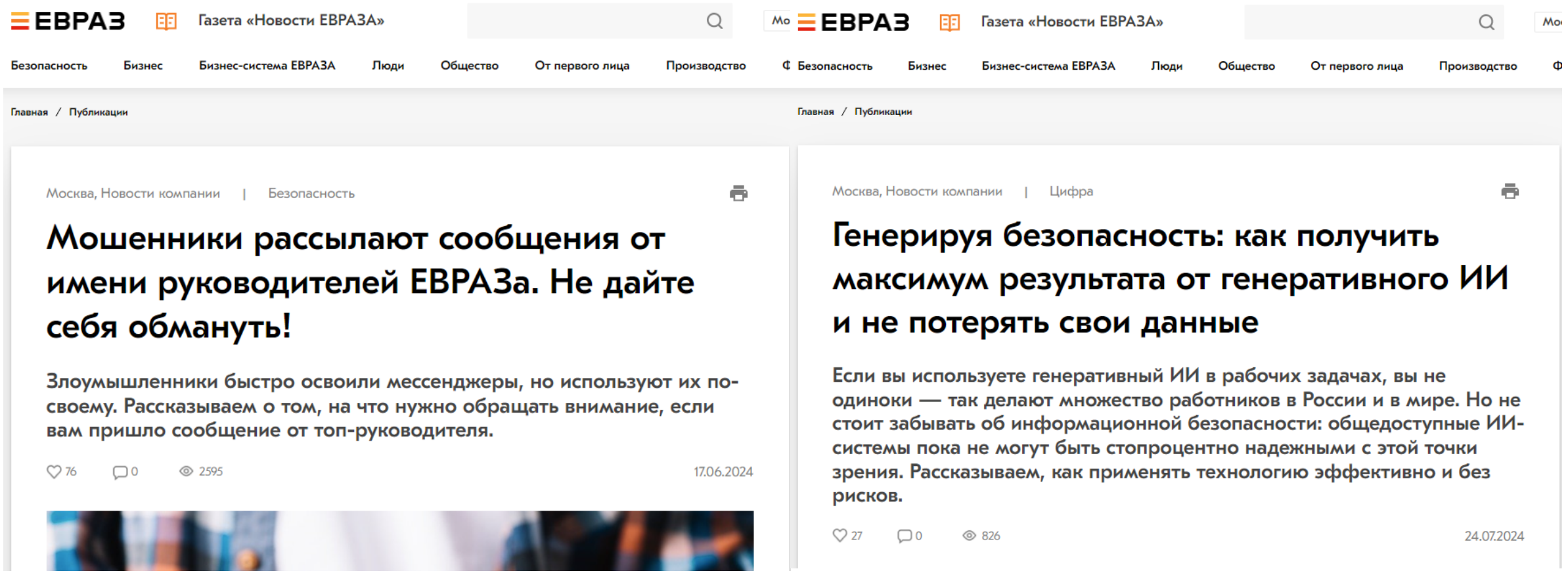
Производитель устанавливает стандартный несложный пароль на все выпускаемые с завода устройства: по умолчанию пароль администратора чаще всего: «admin:admin» и подобные «1234» цифровые последовательности.

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.

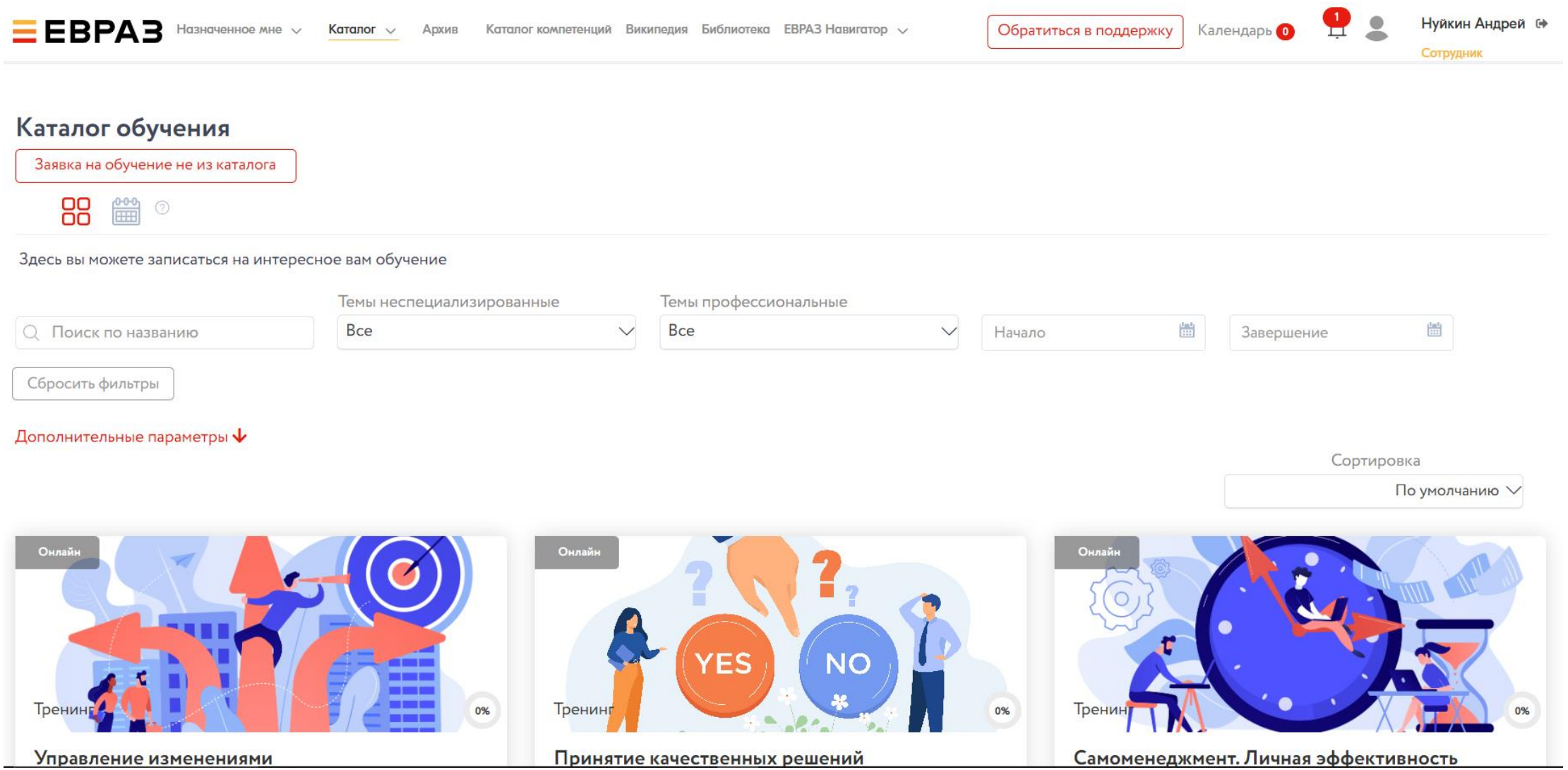
Активация входа в сеть WIFI с помощью протокола WPS (Wi-Fi Protected Setup) – это когда вы вводите секретный ПИН-код, напечатанный производителем на нижней стороне устройства, и получаете доступ, делает возможным взлом за несколько часов с помощью перебора всего лишь 11000 вариантов.

Регулярные новости на портале

ЕВРАЗ



На самом деле все не так сложно

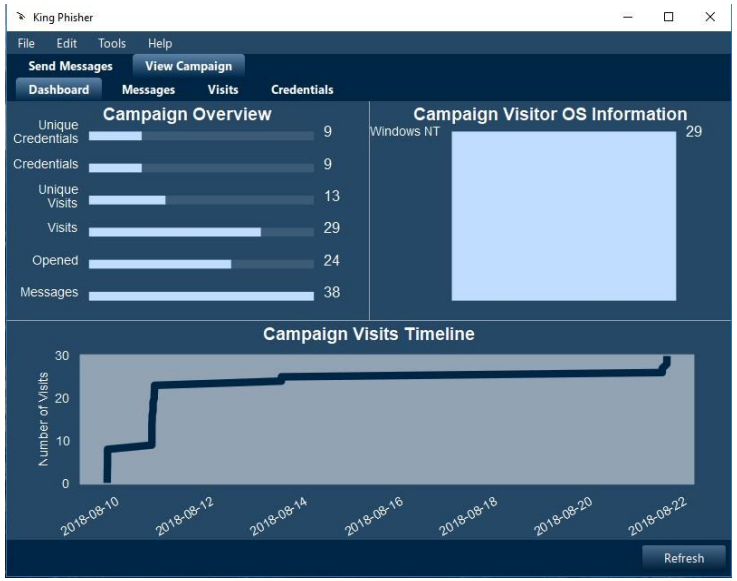


Ролики на Корпоративном ТВ

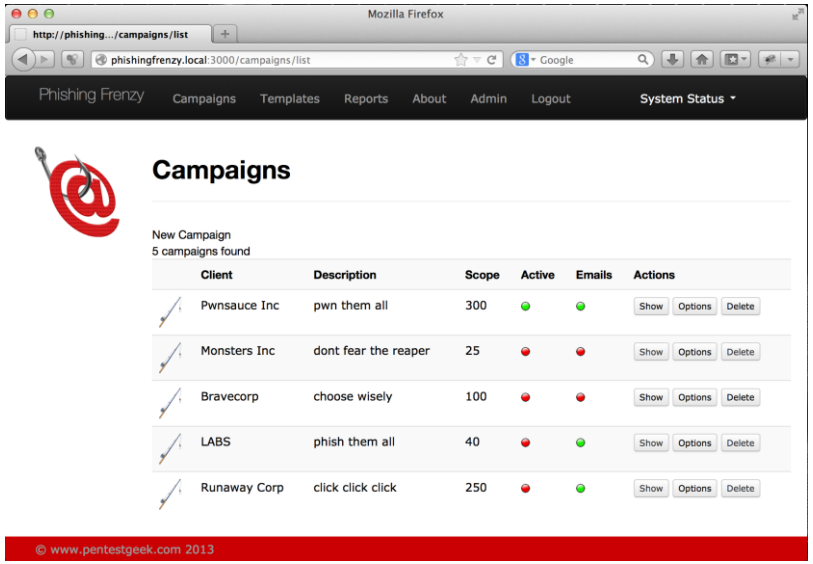
Как провести практическое обучение

ЕВРАЗ

KING PHISHER



PhishingFrenzy



Масштабы охвата

Рассылка осуществляется сотрудникам ЕВРАЗ, управляемых предприятий Москвы, Урала, Сибири, Южных регионов России за исключением ТОП менеджеров.

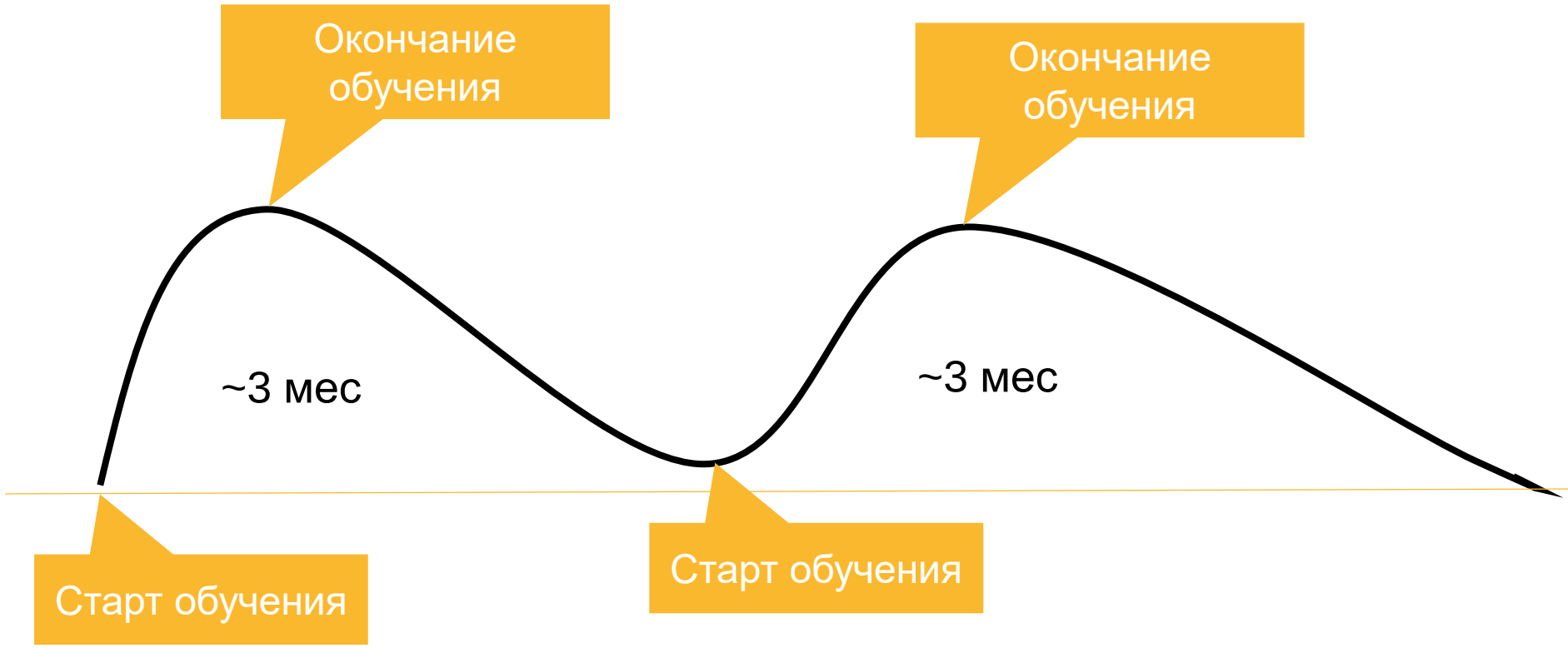
Результаты обучения

ЕВРАЗ

МАЙ 2024

19 тыс. Писем отправлено	(Пусто) Не доставленные письма	19 тыс. Доставленные письма
498 Заявки по Кампаниям	1012 Посетили сайт	685 Пароли
2,61% Процент заявок	5,3% Процент посещения сайта	3,59% Процент паролей

Как реагируют пользователи после обучения



ЕВРАЗ

1. Нужно постоянно работать с пользователями по повышению их осведомленности в области ИБ.

2. Практические занятия лучше теоретических.

3. Добиться 100% защиты не получится, но нужно охватить максимально возможную аудиторию.

ЕВРАЗ

Обучайте пользователей

Сделайте завтра простую рассылку по сотрудникам с правилами ИБ

Андрей Нуйкин
CISA, CISM
АРСИБ
RuSCADASec Coin #29

+7(495) 363-19-60

Andrey.nuykin@evraz.com

www.evraz.com