Киберграмотность не выходя из дома

Антивирусная лекция

Денис Баринов,
руководитель
Kaspersky Academy
academy.kaspersky.ru

kaspersky

Обсудим сегодня

- Безопасность, удаленка и COVID-19: новые угрозы
- Что сделать прямо сейчас, чтобы быть в безопасности в киберпространстве

КАК COVID-19 ВЛИЯЕТ НА СТИЛЬ РАБОТЫ РОССИЯН

Исследование «Лаборатории Касперского»*

22%

стали больше работать

используют личную почту для решения рабочих вопросов

59%

могут чаще бывать с семьей и больше времени посвящать личным делам

56%

55%

общаются по работе в мессенджерах, не одобренных IT-отделами

58%

стали больше читать новостей

читают новости онлайн на устройствах, которые используют для работы

71%

*Исследование «Влияние COVID-19 на стиль работы» проведено «Лабораторией Касперского» апреле 2020 года. Опрошено 6016 сотрудников по всему миру.

51%

работников смотрят контент для взрослых и работают с одних и тех же устройств

К чему это приводит - ошибки сотрудников слишком дорого обходятся бизнесу – даже в «мирное» время

14,3 млн р.

для крупных предприятий

Средний ущерб от успешной атаки, в т.ч. вызванной неумышленными ошибками сотрудников *

4,3 млн р.

для сегмента СМБ

Средний ущерб от успешной атаки, в т.ч. вызванной неумышленными ошибками сотрудников *

33%

российских организаций

Хотя бы раз за год столкнулись с инцидентами, связанными с ненадлежащим использованием ИТ-ресурсов сотрудниками *

до $400

на сотрудника за год

Средние потери компаний от фишинга (без учета прочих векторов атак) **

* *Исследование «Информационная безопасность бизнеса», «Лаборатория Касперского», весна 2018.*
** *Calculations based on Ponemon Institute, "Cost of Phishing and Value of Employee Training", August 2015.*

Какие риски возникают при переходе на удаленку?

- Незащищенные wi-fi сети
- Использование личных устройств для работы
- Широкое использование видеоконференций
- Использование неодобренных IT-службой программ и сервисов
- Доступ семей к рабочим данным
- Интернет-мошенники, спекулирующая на ситуации

Когда надежный пароль становится фактором национальной безопасности

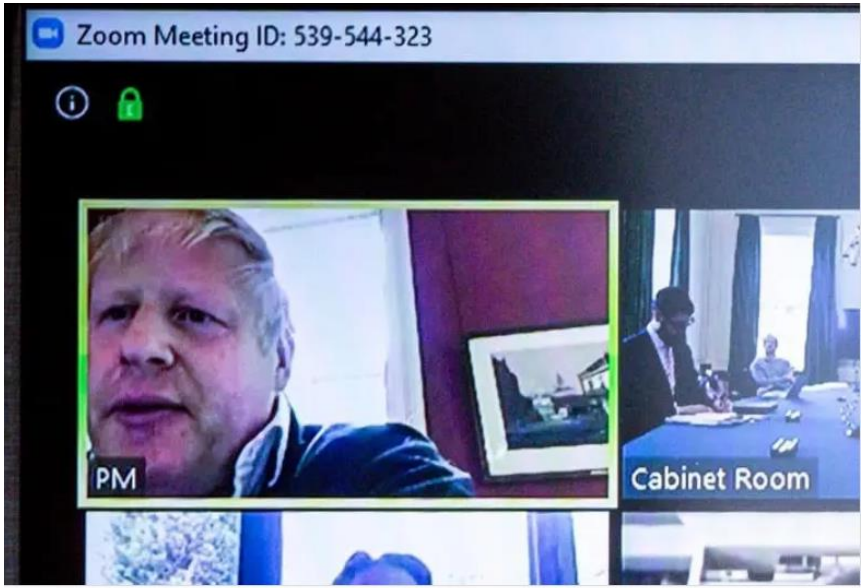
Используйте надежный пароль ко всем средствам деловой коммуникации – и не разглашайте даже части конфиденциальных данных

Good news for anyone who was hoping to join the meeting but had mislaid the Zoom meeting ID.

But bad news for any mischief makers hoping to take advantage – the Zoom meeting is password-protected. Thank heavens for that.

Let's hope it's a strong password, that's hard to guess.

Boris Johnson inadvertently reveals the UK Government's Cabinet Meeting Zoom I.D. on Twitter



Boris Johnson's Zoom meeting. Click for larger version

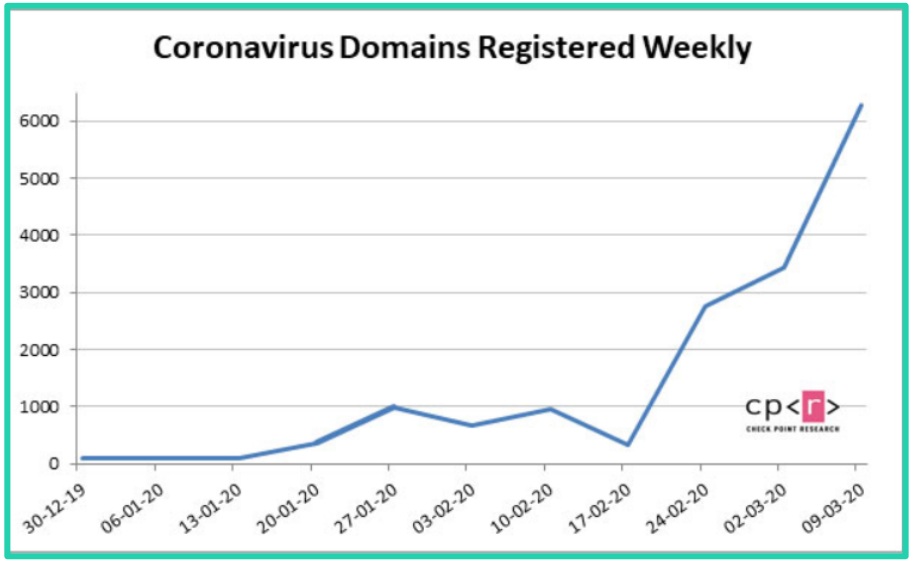
Киберпреступники эксплуатируют обеспокоенность пользователей

19%

всех связанных с коронавирусом доменов подозрительны

0,8%

- однозначно вредоносны




```
2020-3-18,11:48:56.182348,www.covid19-entreprises90.fr
2020-3-18,11:49:53.129553,*.uks-covid19-tellushow-dev-ase.p.azurewebsites.net
2020-3-18,11:51:09.231271,www.coronavirusdisease19.site
2020-3-18,11:56:15.431098,coronavirus-crisis.co.uk
2020-3-18,11:56:24.218537,covid19.greencloudsolution.com
2020-3-18,11:56:27.975749,phlcovid-19fund.org
2020-3-18,11:57:01.928890,*.ntucoronavirusinformation.info
2020-3-18,11:57:16.637661,www.covid19norge.no
2020-3-18,11:57:19.273386,coronavirus-online-monitor.wcg-case.ru
2020-3-18,11:59:42.859371,coronavirus.allmentalhealth.org
2020-3-18,11:59:58.225036,covid19.nirmatacreative.com
2020-3-18,12:00:51.783705,www.covid19recovery.net
2020-3-18,12:02:52.554491,covid19.windwardapps.com
2020-3-18,12:03:07.166397,covid19.windwardapps.com
2020-3-18,12:04:00.945511,covid19.dhis2nigeria.org.ng
2020-3-18,12:04:08.562179,coronavirus-wirtschaft.ch
2020-3-18,12:06:32.025836,covid19cincy.org
2020-3-18,12:06:39.999103,hammamlif-covid19.com
2020-3-18,12:07:55.312766,coronavirus-prognoz.ru
2020-3-18,12:08:09.995917,coronavirus-hilfe.ch
```

Вредонос-шпион AZORult эмулирует карту Университета Джона Хопкинса (через .exe-файл)

Троян собирает информацию, хранящуюся в браузерах: cookies, история посещений страниц, идентификаторы пользователей, пароли, ключи от криптовалютных кошельков

Защита: ставить антивирус и не ставить exe-файлы

Приложение COVID19 Tracker считывает пароль от телефона и блокирует вход, требуя выкуп

Бэкдор, вымогатель

Защита:

- бэкап
- не ставить неизвестные приложения
- отдельно защищать корпоративную информацию на устройствах

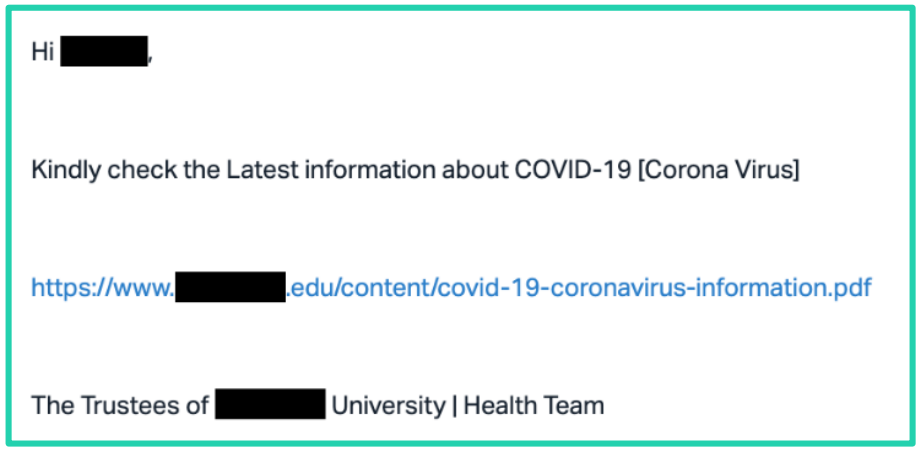
Письмо якобы от руководства предлагает ознакомиться с информацией – и ворует учетные записи Microsoft

Фишинг
Воровство аккаунтов

Защита:
- умение распознавать фишинг
- подозрительность при вводе логина и пароля

20 тысяч

студентов и сотрудников американских вузов получили фишинговое письмо якобы от руководства с просьбой ввести логин и пароль от учетной записи Microsoft

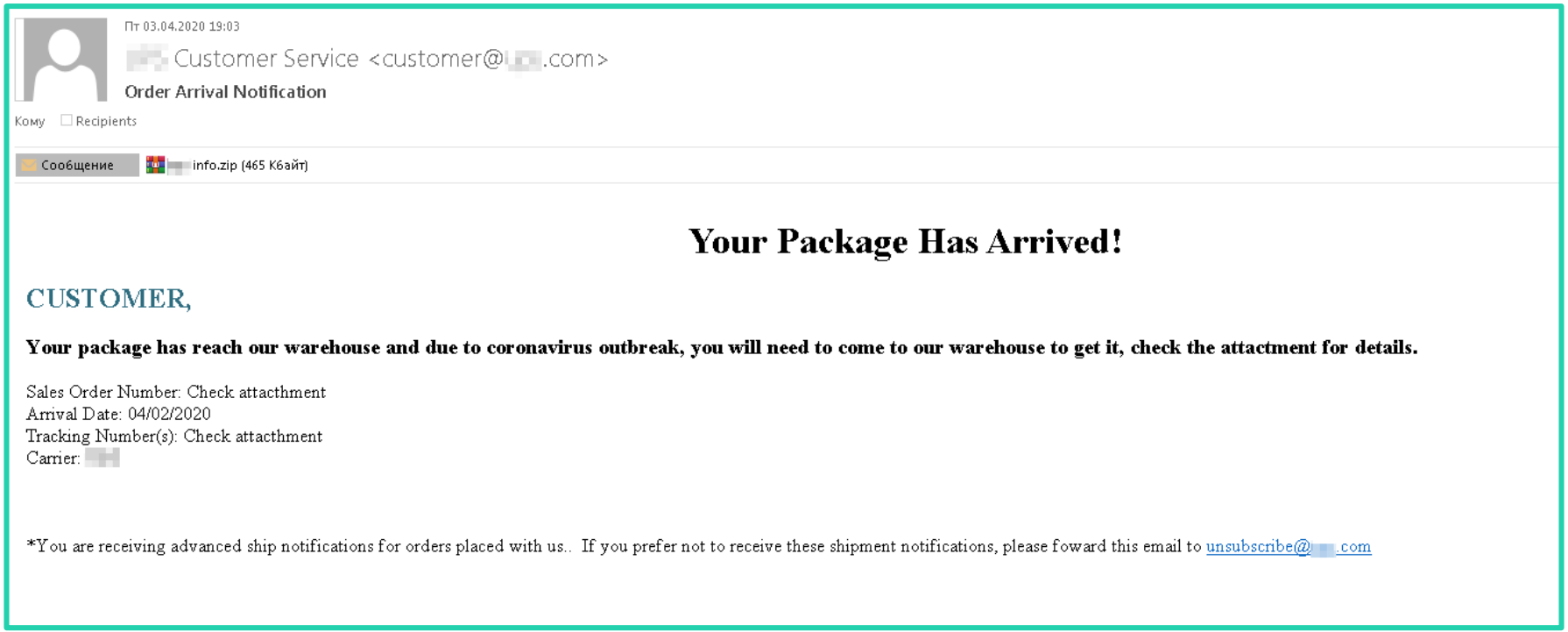

Hi [redacted],

Kindly check the Latest information about COVID-19 [Corona Virus]

https://www.[redacted].edu/content/covid-19-coronavirus-information.pdf

The Trustees of [redacted] University | Health Team

Кроме того – подделка писем от служб доставки….



Пт 03.04.2020 19:03

Customer Service <customer@[redacted].com>

Order Arrival Notification

Кому Recipients

Сообщение info.zip (465 Кбайт)

Your Package Has Arrived!

CUSTOMER,

Your package has reach our warehouse and due to coronavirus outbreak, you will need to come to our warehouse to get it, check the attactment for details.

Sales Order Number: Check attacthment
Arrival Date: 04/02/2020
Tracking Number(s): Check attacthment
Carrier: [redacted]

*You are receiving advanced ship notifications for orders placed with us.. If you prefer not to receive these shipment notifications, please foward this email to unsubscribe@[redacted].com

Кроме того – подделка писем от служб доставки….

Ср 01.04.2020 0:37

EXPRESS <shipping@.com>

Cargo Arrival Notice!!

Кому .com

Сообщение | Arrival Notice.jpg.ace (24 Кбайт)

Our Dear Customer ,

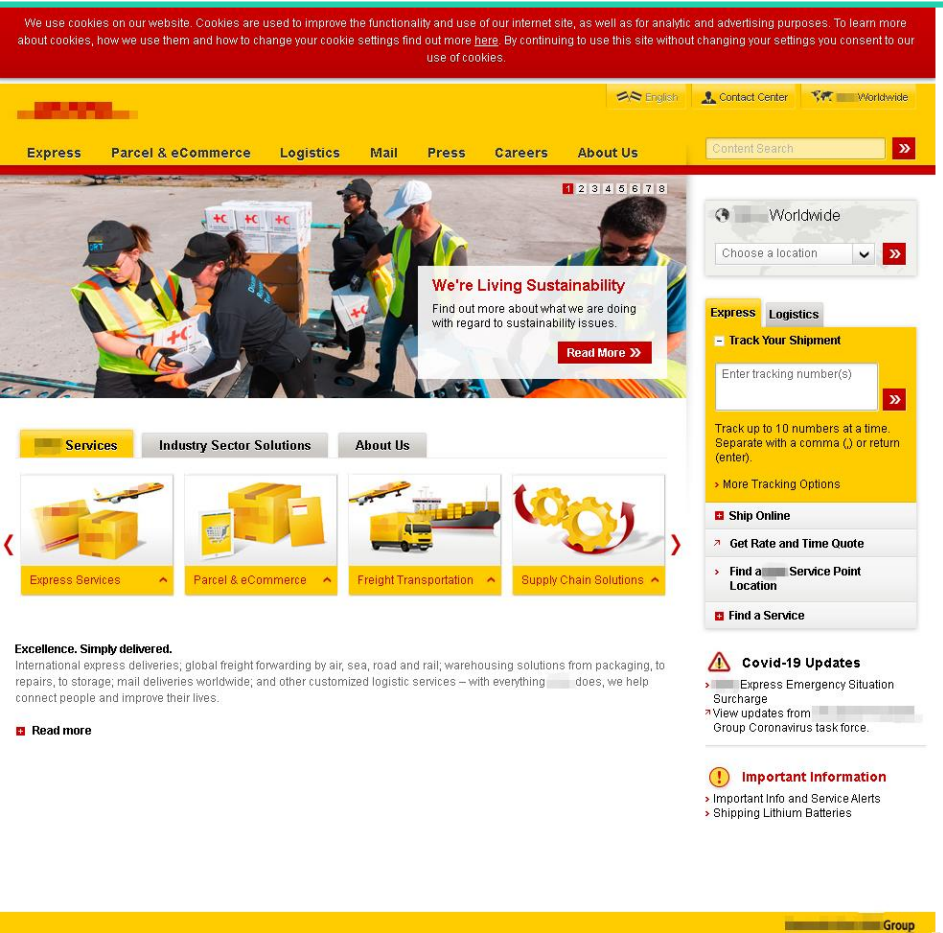
Urgent__ Your shipment arrived our regional Office on 30th, however the details provided for dispatch are incomplete pls check.

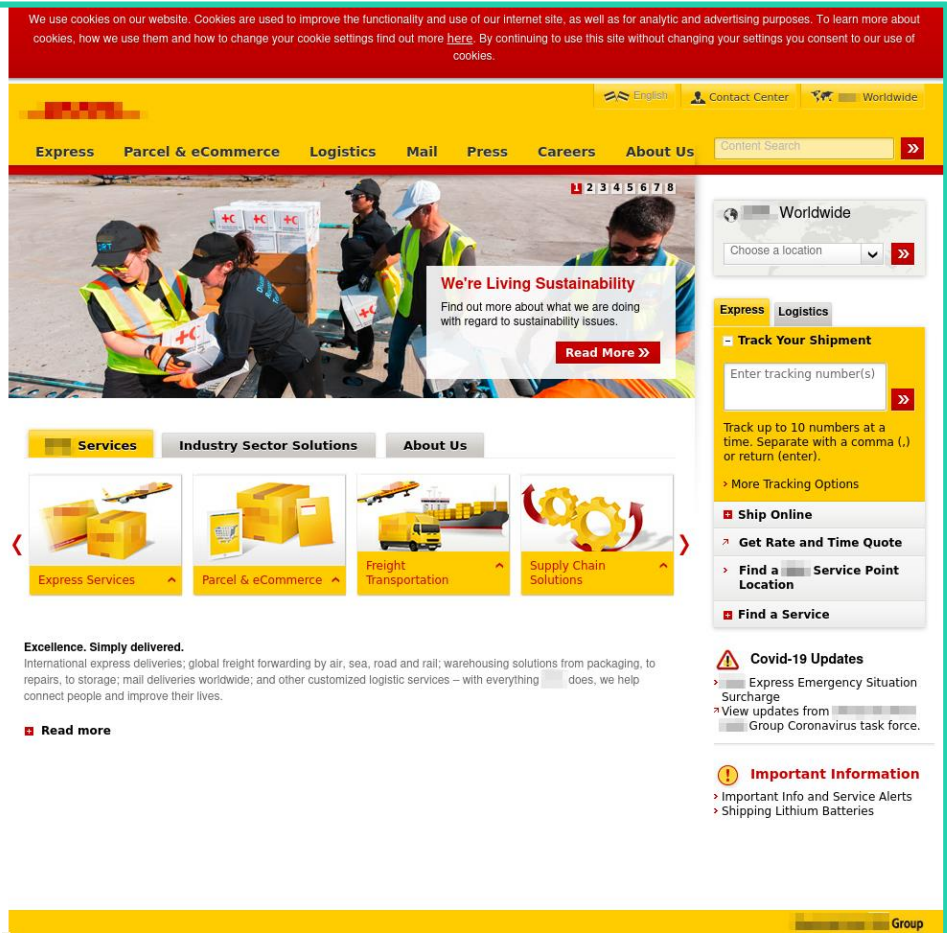
kindly see attach document and resend us corrected details for Tracking your address, to enable us proceed with Dispatch before goverment lock down, prior to the Coronavirus pandemic precautionary major.

Yours Sincerely,

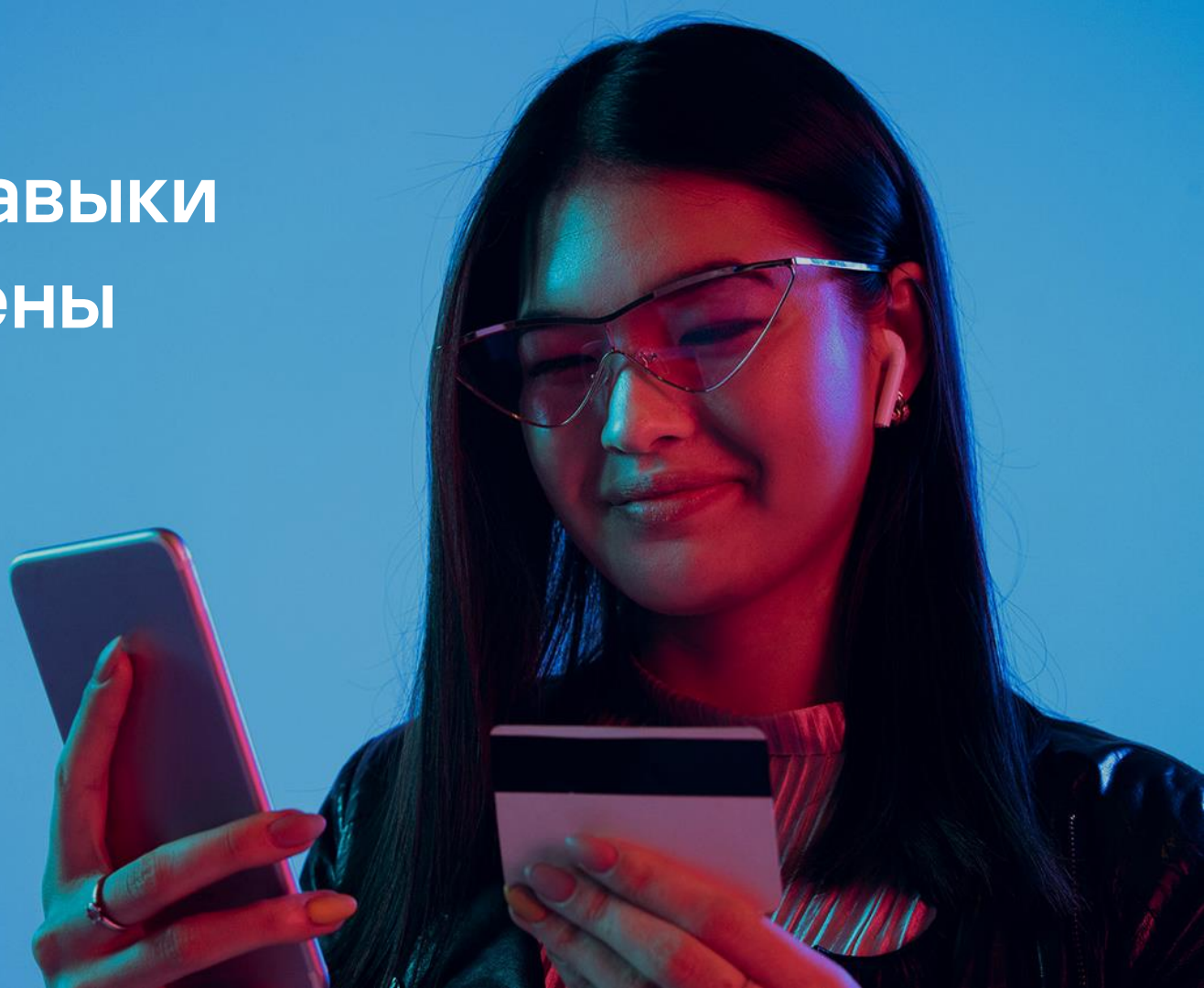
Customer Service Officer
EXPRESS
support@worldwide.inc

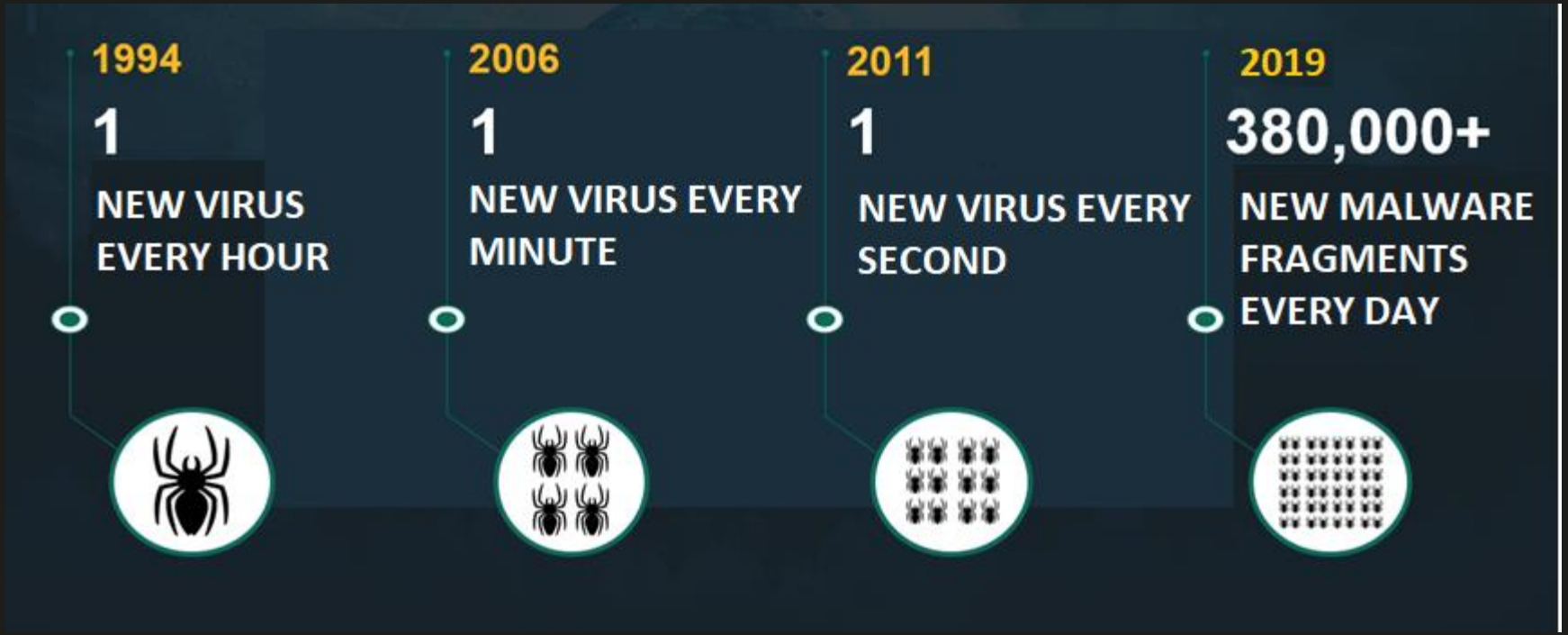
....и даже целых сайтов





Простые навыки кибергигиены




1994
1
NEW VIRUS EVERY HOUR
2006
1
NEW VIRUS EVERY MINUTE
2011
1
NEW VIRUS EVERY SECOND
2019
380,000+
NEW MALWARE FRAGMENTS EVERY DAY

Сделать:

- Используйте зашифрованное по стандарту **WPA2 соединение**
- Установите на доступ к роутеру сложный, **12-значный пароль**
- Используйте **двухфакторную аутентификацию** на важных ресурсах

Проверить:

- Вы знаете, что это такое и как проверить, **какой стандарт использует сеть?**
- Вы знаете, где и как поменять **пароль** (и что такое **роутер**)?
- Важные **ресурсы** имеют двухфакторную аутентификацию? Вы умеете ее устанавливать?

Сделать:

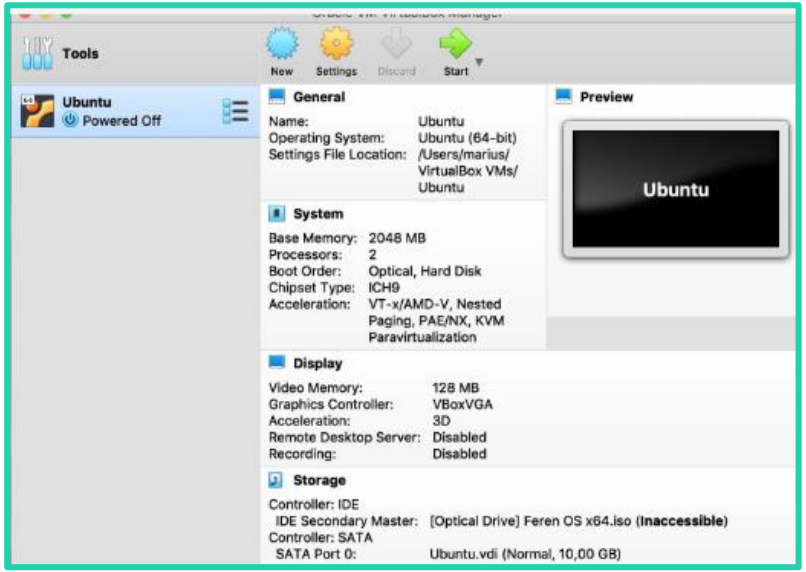
- Создайте для каждого пользователя (в т.ч. членов семьи и/или гостевую) **отдельную учетную запись**
- Защитите свою учетную запись **надежным паролем**

Проверить:

- Вы сможете создать **гостевые учетные записи** на рабочих компьютерах? А на личных?
- Вы знаете, что такое **надежный пароль**? Умеете их составлять? А запоминать?
  (или повесите бумажку с паролем на холодильник?)

Сделать:

- Установить ☺ (Например, Virtual box)
- Если работаете на личном компьютере – ставьте **виртуальную машину**!



Сделать:

- Проверьте на **адрес отправителя** и **текст** (грамотность, формат, контекст)
- Не открывайте **вложения** в письмах от служб доставки
- Осторожнее с письмами про **коронавирус**
- Не предоставляйте в ответ на письмо **никаких данных**
- Пользуйтесь **надежным защитным решением,** которое распознает вредоносное вложение и заблокирует фишинговый сайт

Проверить:

- Вы умеете определять фишинговые письма? А **спирфишинг**?
- Вы можете распознать и противостоять методам **социальной инженерии?**

Сделать:

- Проверяйте, не накопились ли неавтоматические обновления, и **своевременно** устанавливайте их!
- **Перезапускайте компьютер,** чтобы автоматические обновления начали действовать

Проверить:

- Расписание **автоматических обновлений** действует? А на личных компьютерах?
- Вы понимаете **важность обновлений?** Держите в голове необходимость проверки?
- Вы понимаете, что перезагрузка компьютера точно нужна **чаще раза в месяц?**

Другие важные принципы безопасности

1. Обеспечьте наличие и актуальность антивируса, в т.ч. на используемых для работы **личных ресурсах. Регулярно** сканируйте весь компьютер
2. Создавайте резервные копии
3. Используйте VPN
4. Используйте сложные пароли. Регулярно их обновляйте. Используйте менеджер паролей
5. Используйте разные браузеры для работы и личных надобностей. Не устанавливайте **плагины** в браузеры
6. Любую служебную информацию размещайте только **на корпоративных ресурсах**. В крайнем случае - на личных ресурсах (Google Drive и пр.) **с паролем**

..И о безопасности платежей

Одна смешная история (конечно же, это не про вас)

CARD POST

Another notable story happened in 2014. Twitter user Alyssa Alcantar boasted about getting a new debit card, posting a picture of it with the caption: "Finally got my debit card! Love the blue."

A couple people in the comments immediately asked what the three numbers were on the back, and Alyssa, without skipping a beat, answered: "The back code of my card is 388 why is everyone asking? smh." That same day, all the money Alyssa managed to save there was withdrawn from the card.

It's funny, but Alyssa didn't understand what happened, and after she got a replacement card, she immediately posted it on the same page, albeit without the CVC/CVV code.

Немного статистики* (2019)

70%

мошенничеств происходит с использованием методов социальной инженерии

24 млрд. $

убытки от махинаций с кредитными картами**

15%

снизился объем мошеннических CNP-транзакций

73%

снизился объем POS и ATM мошенничеств

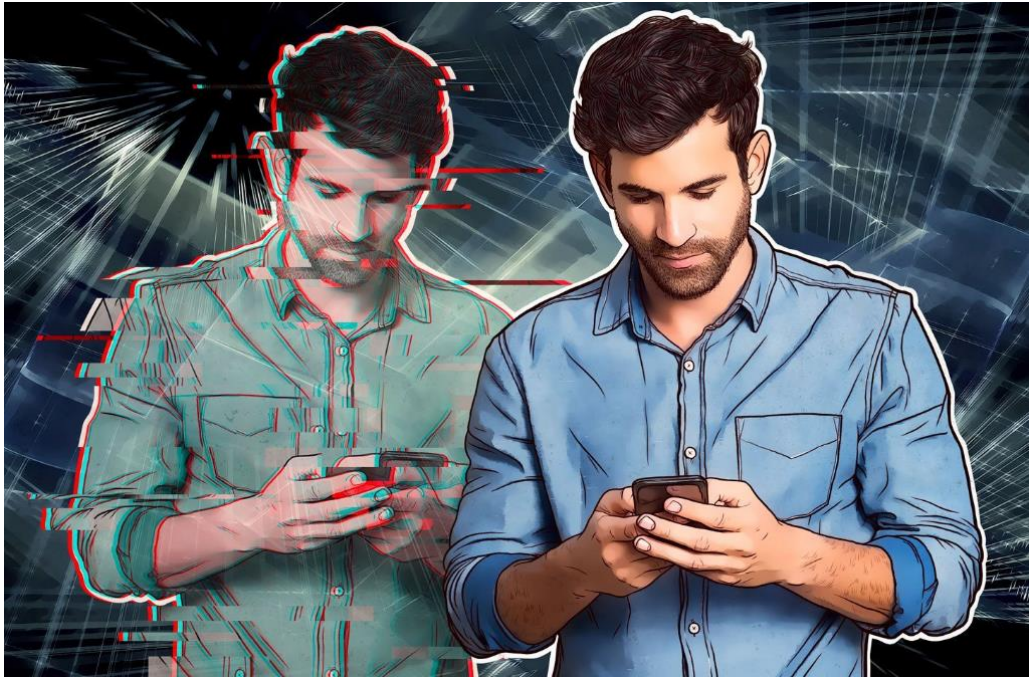
* - https://www.kaspersky.ru/about/press-releases/2019_rayffayzenbank-i-laboratoriya-kasperskogo-proanalizirovali-trendy-kartochnogo-froda

** - The Nilson Report 2018

Лучше один раз увидеть...

Зачем злоумышленникам данные вашей карты?

- $$$
- Использовать данные для нелегальных операций
- Продать данные карты

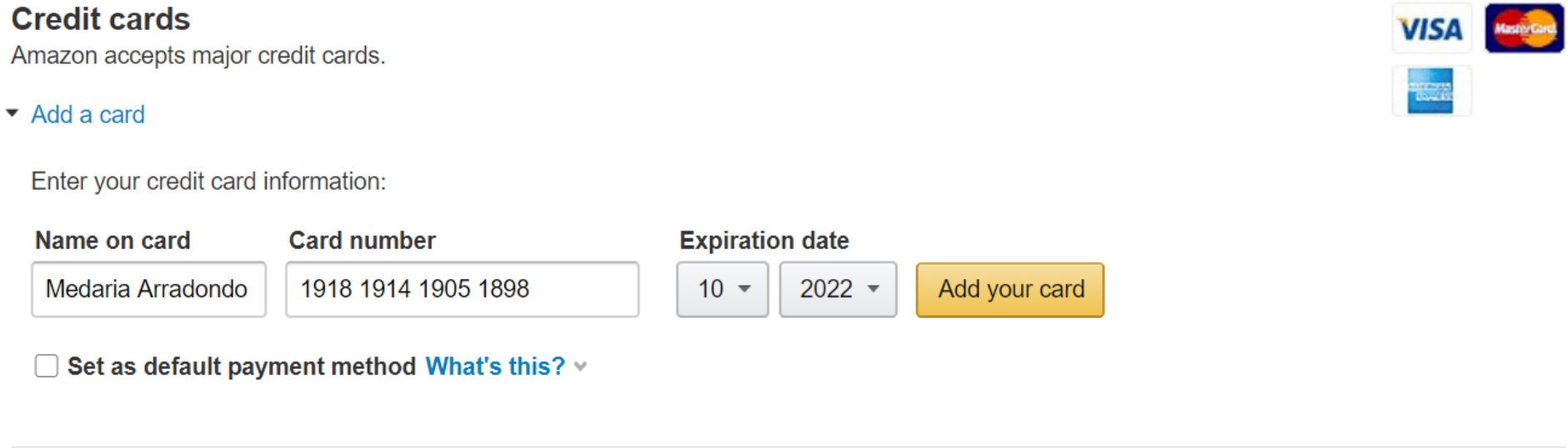


Сколько данных нужно, чтобы совершить покупку по вашей карте?

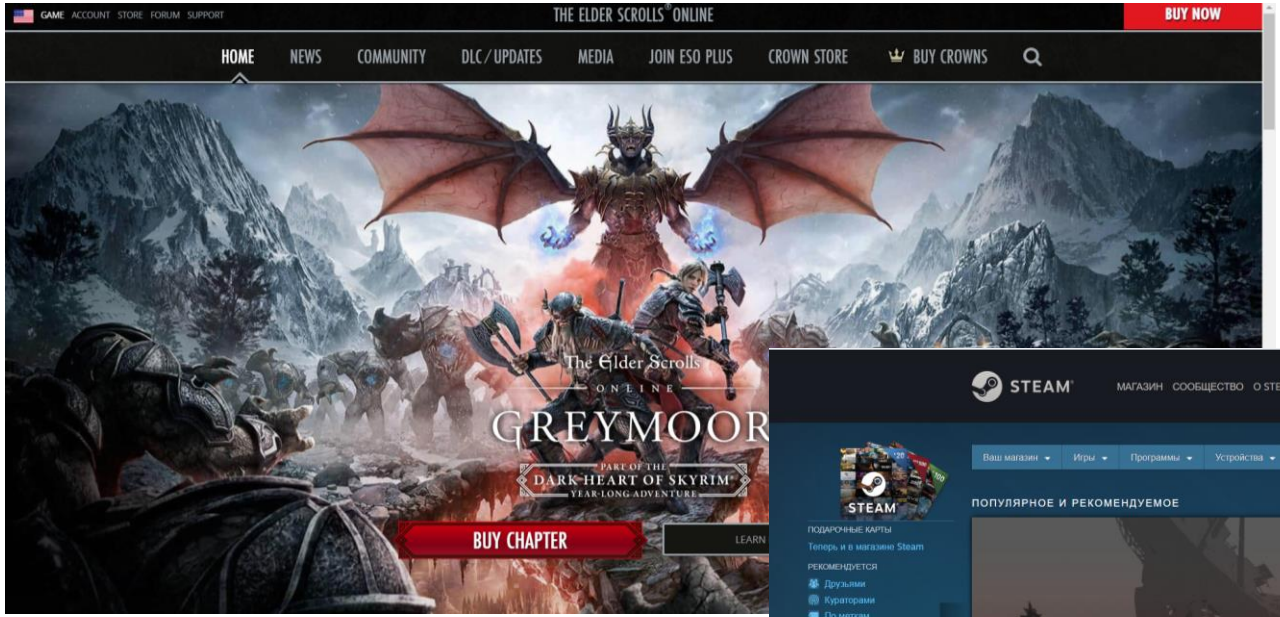
Сколько данных нужно, чтобы совершить покупку по вашей карте?

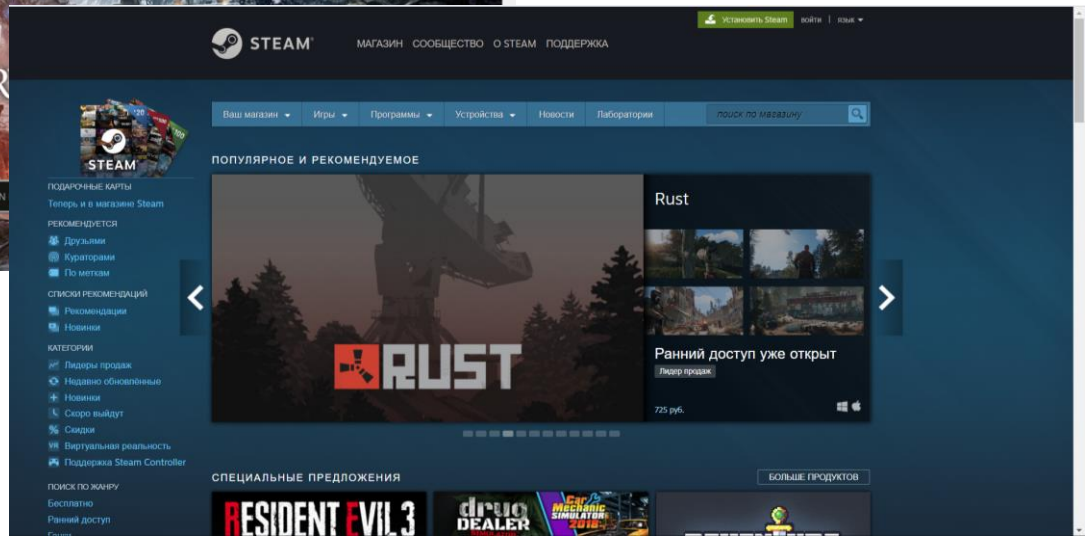
Ничего	Почти ничего	Заплатить в некоторых интернет-магазинах	Забронировать отель или авто, привязать карту к Гугл-плею, заплатить на Литресе	Заплатить где угодно в интернете, сделать любой платеж или перевод
Номер карты	Номер карты	Номер карты	Номер карты	Номер карты
	Имя и фамилия	Имя и фамилия	Имя и фамилия	Имя и фамилия
		Срок действия	Срок действия	Срок действия
			Код безопасности	Код безопасности
				Код из смс

Для привязки карты к аккаунту Amazon не нужен CVV



Для покупок на игровых платформах часто не требуется код подтверждения





Примеры атак:

- Кража учетной записи интернет-банка
- Привязка карты к магазину приложений
- Оплата картой в онлайн-магазинах
- Проведение транзакций через звонок/смс клиенту банка

На каких сайтах можно платить?

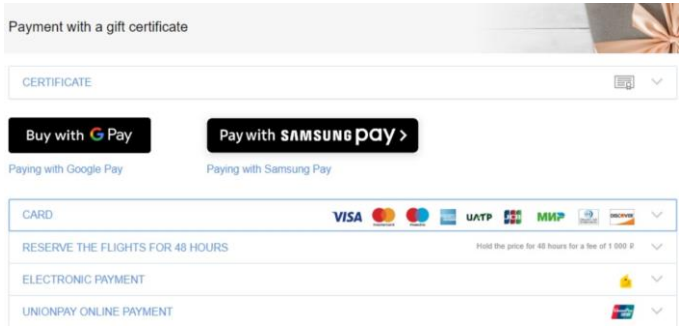
1

2

MasterCard SecureCode. Verified by VISA AMERICAN EXPRESS

SafeKey Diners Club INTERNATIONAL ProtectBuy

3



- Платежные системы (PayPal, Qiwi, WebMoney)
- Но проверяя! Платежных систем много (Paymill, Stripe, Skrill, Paymaster, GoCardless…)
- Виртуальной картой
- Курьеру☺

- **…и никому не пересылать никаких данных банковской карты (кроме номера)!**

Итак

1. Отдельная карта для покупок онлайн
2. Проверяйте подлинность интернет-магазинов
3. Только бесконтактная оплата
4. Установите антивирусное ПО на телефон (Android – must)
5. Используйте приложение для определения номеров
6. Не передавайте данные, не сообщайте коды подтверждения
7. Не публикуйте перс данные (номер телефона)
8. Не используйте одинаковые пароли для онлайн-сервисов, особенно – для клиент-Банка

...А что в итоге


Как менять пароль на роутере?
Что такое роутер, Наташ
Ну ее эту двухфакторную аутентификацию
У меня вообще нет WPA2, Наташ

Дополнительно

Бесплатные курсы по кибербезопасности

Пример:
«Безопасность в жизни и бизнесе»
kas.pr/free-course

Берегите себя

Kaspersky Academy

kaspersky.com/awareness academy@kaspersky.com awareness@kaspersky.com

kaspersky