Знание.
Государство

ЦИФРОВАЯ ГИГИЕНА И ЛИЧНАЯ БЕЗОПАСНОСТЬ В ИНТЕРНЕТЕ

Российское общество «Знание»

2024

СТАТИСТИКА УТЕЧКИ ДАННЫХ В РОССИИ

- 140 утечек
- 702 млн записей о россиянах

- 95 крупных баз данных
- 1,12 млрд записей о россиянах
- в результате кибератак более 80% утечек

Исследование проводила компания InfoWatch

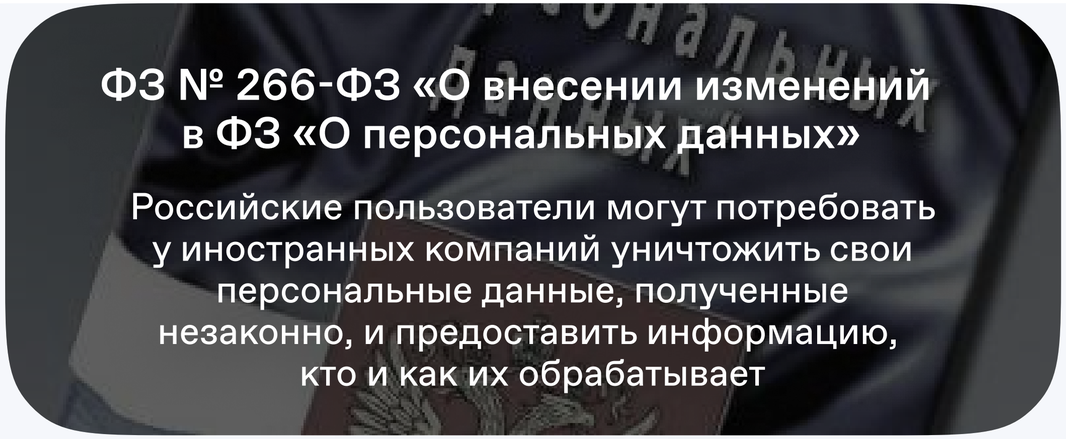
КАК КОМПАНИИ БОРЮТСЯ С УТЕЧКОЙ ДАННЫХ

59% провели для сотрудников обучение основам информационной безопасности

27% внедрили системы защиты от кибератак

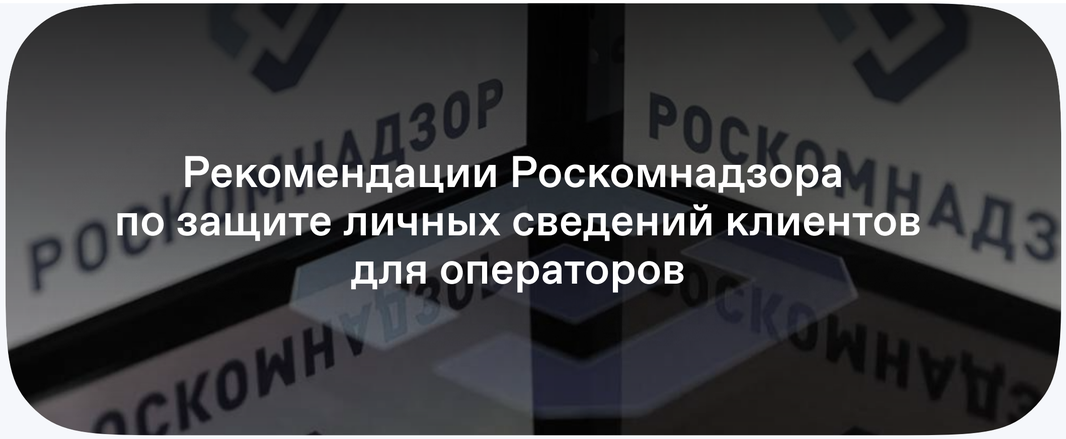
17% установили DLP-системы, которые предотвращают утечку конфиденциальных данных из корпоративной сети

КАК ГОСУДАРСТВО ДЕЛАЕТ ЦИФРОВОЕ ПРОСТРАНСТВО БЕЗОПАСНЫМ



ФЗ № 266-ФЗ «О внесении изменений в ФЗ «О персональных данных»

Российские пользователи могут потребовать у иностранных компаний уничтожить свои персональные данные, полученные незаконно, и предоставить информацию, кто и как их обрабатывает



Рекомендации Роскомнадзора по защите личных сведений клиентов для операторов

Поручение Президента России В.В. Путина о переходе отечественных государственных компаний на российские операционные системы и офисные пакеты к началу 2025 года

Запрет на использование iPhone и iPad для служебных целей сотрудникам российских министерств и ведомств, переход на модели российских производителей

ИНТЕРНЕТ-МОШЕННИЧЕСТВО —

один из способов незаконного получения личных данных (паролей, реквизитов банковских карт) путем предоставления человеку неверной информации, фиктивных угроз, вымогательства

Самые распространенные схемы мошенничества:

- Обзвон граждан от имени правоохранительных органов или банков
- Создание фальшивых (фишинговых) сайтов для получения доступа к конфиденциальным данным пользователей
- Рассылка писем о «крупном выигрыше» по электронной почте
- Фальшивые сайты благотворительных организаций/туроператоров/ авиакомпаний
- Предложение выгодного заработка на подозрительных интернет-ресурсах
- Взлом личных аккаунтов пользователей и рассылка сообщений
- Лотереи, викторины, конкурсы, где нужно заплатить «налог на выигрыш» или «комиссию за доставку приза»

СТАТИСТИКА ФИШИНГОВОГО МОШЕННИЧЕСТВА

Фишинговые рассылки приходят не менее двух раз в месяц. Такие письма обычно содержат предложения выгоды, быстрого заработка.

48% пользователей получили информацию об акциях с высокой доходностью

28% пользователей получили сообщения о больших скидках на популярные товары

~12% пользователей получили письма о неоплаченных штрафах и задолженностях

Цели злоумышленников:

35,8% случаев получить доступ к данным банковских карт

24,4% случаев узнать паспортные данные

17,9% случаев выяснить логины и пароли от разных сервисов

Опрос интернет-пользователей произведен компанией «МТС Red»

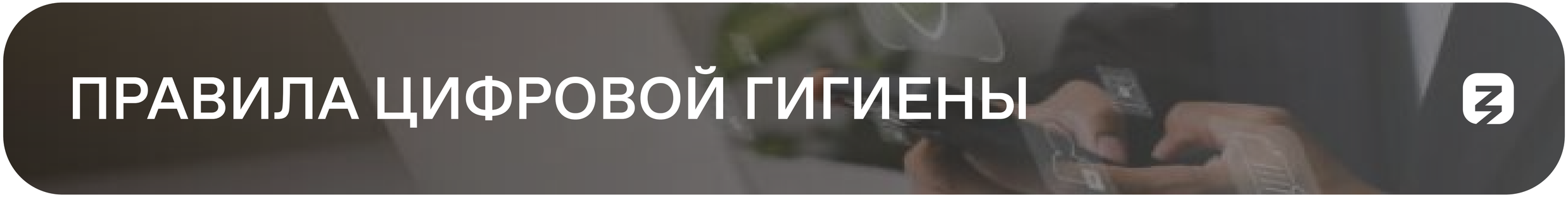
ПРАВИЛА ЦИФРОВОЙ ГИГИЕНЫ

- Не давайте свой телефон незнакомым людям под предлогом срочного звонка
- Устанавливайте длинные и надежные пароли, усиленные биометрией и двухфакторной аутентификацией. Регулярно меняйте их
- Устанавливайте оригинальные пароль, PIN-код и другие виды защиты для блокировки компьютера и телефона
- Выполняйте регулярное резервное копирование данных на внешний жесткий диск
- Избегайте публикации личной информации в соцсетях (номер телефона, фото, домашний и рабочий адреса, номера кредитных и банковских карт, местоположение)

ПРАВИЛА ЦИФРОВОЙ ГИГИЕНЫ

- Не принимайте заявки в соцсетях от незнакомых и сомнительных людей
- При установке нового приложения проверяйте, к каким данным на вашем устройстве у вас запрашивают разрешение
- Регулярно обновляйте программы, приложения и операционные системы. Старые версии могут быть более уязвимы для атак
- Отписывайтесь от ненужных рассылок и подписок
- Внимательно открывайте электронные письма с неизвестных адресов, не переходите по объявлениям и ссылкам, которые обещают скидки, призы и денежные выигрыши

ПРАВИЛА ЦИФРОВОЙ ГИГИЕНЫ



- При использовании публичных сетей Wi-Fi будьте аккуратны при открытии мобильного банка. Злоумышленники часто используют такие сети в своих целях
- Контролируйте покупки в интернете. Под видом онлайн-магазина могут быть мошенники
- Используйте сетевой экран. Он предотвращает несанкционированный доступ к вашим веб-сайтам, почте, паролям и другой информации
- При продаже старых гаджетов отформатируйте и очистите жесткий диск
- Используйте хорошее антивирусное программное обеспечение, регулярно проводите автоматическую проверку устройства на вредоносные программы

РАСПОЗНАТЬ ФЕЙК — ОДНО ИЗ ГЛАВНЫХ ПРАВИЛ ЦИФРОВОЙ ГИГИЕНЫ

На что необходимо обратить внимание:

насколько эмоционален заголовок

какие источники у новости и насколько они авторитетны

какое качество у фотографий и видео

новость содержит факты или субъективный взгляд

есть ли опечатки и ошибки в тексте

корректен ли адрес домена (защищенный адрес всегда начинается с https://)

НАДЕЖНОСТЬ ПАРОЛЯ И НЕОБХОДИМОЕ ВРЕМЯ ДЛЯ ЕГО ВЗЛОМА (БРУТФОРС)

Количество символов	Только числа	Буквы в нижнем регистре	Буквы в нижнем и верхнем регистре	Числа и буквы в нижнем и верхнем регистре	Числа, буквы в нижнем и верхнем регистре, символы
4	мгновенно	мгновенно	мгновенно	мгновенно	мгновенно
5	мгновенно	мгновенно	мгновенно	мгновенно	мгновенно
6	мгновенно	мгновенно	мгновенно	мгновенно	мгновенно
7	мгновенно	мгновенно	2 сек	7 сек	31 сек
8	мгновенно	мгновенно	2 мин	7 мин	39 мин
9	мгновенно	10 сек	1 час	7 часов	2 дня
10	мгновенно	4 мин	3 дня	3 нед	5 мес
11	мгновенно	2 часа	5 мес	3 года	34 года
12	2 сек	2 дня	24 года	200 лет	3 тыс. лет
13	19 сек	2 мес	1 тыс. лет	12 тыс. лет	202 тыс. лет
14	3 мин	4 года	64 тыс. лет	750 тыс. лет	16 млн лет
15	32 мин	100 лет	3 млн лет	46 млн лет	1 блн лет
16	5 часов	3 тыс. лет	173 млн лет	3 блн лет	92 блн лет
17	2 дня	69 тыс. лет	9 блн лет	179 блн лет	7 блр лет
18	3 недели	2 млн лет	467 блн лет	11 блр лет	438 блр лет

ОБЩИЕ РЕКОМЕНДАЦИИ

- Доверяйте только проверенным источникам
- Дайте новостям время: перепроверяйте информацию, добытую «по горячим следам»
- Проверяйте факты самостоятельно в нескольких авторитетных и официальных источниках
- Следите за порталами, которые раскрывают фейки и сообщают о них
- Проверяйте видео на дипфейки: следите за артикуляцией говорящего и его мимикой. При любом несовпадении проверьте данную информацию

Знание.
Государство

Благодарим за внимание!

**Станем лучше для вас.
Поделитесь впечатлениями!**