kaspersky



КиберОктябрь 2026

Тема недели: безопасность паролей

9 базовых правил безопасности паролей

Для компании

1

Внедрите корпоративный менеджер паролей: снимите с людей стресс

Требовать от сотрудников помнить десятки сложных паролей и регулярно их менять — верный путь к записным книжкам со шпаргалками или паролям вроде Spring2026!, Summer2026!. Менеджер паролей закрывает этот разрыв: он сам генерирует невзламываемые комбинации, подставляет их в формы авторизации и предупреждает об утечках.

2

Настройте парольные политики и ролевой доступ

Надежность корпоративного периметра не должна зависеть от вдохновения конкретного человека. Если система технически позволяет поставить пароль 123456, кто-нибудь обязательно его поставит. А избыточные права доступа могут превратить компрометацию рядового аккаунта в масштабный инцидент.

3

Отзывайте доступы в день увольнения

«Забытые» учетные записи бывших сотрудников со старыми паролями — любимая лазейка для киберпреступников. Если человек уволился полгода назад, а его пароль от VPN или почты всё еще действует, компания держит парадную дверь открытой.

4

Проводите практические тренировки: покажите, за сколько секунд ломается пароль

До 60% стандартных паролей ломаются автоматизированными программами перебора менее чем за час. Сухие инструкции из регламентов безопасности не меняют привычек, пока человек лично не увидит уязвимость привычной комбинации.

Для каждого сотрудника

5

Один сервис — один пароль: не плодите цифровых близнецов

Использовать один и тот же пароль для рабочей почты, аккаунта в интернет-магазине и сайта с доставкой пиццы — это очень удобно и очень опасно. Достаточно одной утечки (о которой не всегда сообщают публично), чтобы злоумышленники смогли получить доступ ко всему вашему цифровому имуществу.

6

Длина побеждает сложность: забудьте про фокусы вроде «P@ssw0rd!»

Замена буквы «о» на ноль, а «а» на знак «@» не делает пароль неуязвимым — роботы-взломщики знают эти приемы наизусть и подбирают подобные «ребусы» за доли секунды. В криптостойкости решает длина: каждый дополнительный символ увеличивает время подбора по экспоненте. Да и запомнить длинную осмысленную фразу из нескольких слов в разы проще, чем короткий набор спецсимволов.

7

Включите второй замок: 2FA обязательна везде

Даже самый длинный пароль можно подсмотреть через плечо, выманить фишингом или перехватить вредоносной программой. Двухфакторная аутентификация превращает украденный пароль в бесполезную строчку текста: без подтверждающего кода со смартфона злоумышленник просто не попадет внутрь.

8

Пароль — персональная тайна: его не называют даже системному администратору

Настоящей службе техподдержки или системному администратору никогда не нужен ваш пароль — у них есть собственные административные инструменты для управления правами. Если кто-то в чате или по почте просит: «Срочно пришли пароль, мы обновляем базу», — это классическая атака методом социальной инженерии.

9

Не доверяйте пароли встроенной памяти браузера

Кнопка «Сохранить пароль?» в браузере выглядит соблазнительно, но не стоит поддаваться соблазну. Вредоносные программы-стиллеры охотятся именно за хранилищами паролей в браузерах: при заражении устройства они выкачивают все сохраненные учетные данные за пару секунд.

КиберОктябрь 2026

Подробнее

www.kaspersky.ru

© 2026, АО «Лаборатория Касперского». Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

#kaspersky
#активируйбудущее