Битрикс24

Как обезопасить сотрудников от кибермошенников

7 правил, как обезопасить сотрудников от кибермошенников

Данные — один из самых ценных активов компании. Любая утечка или взлом могут нанести бизнесу финансовый и репутационный урон. Нередко уязвимым звеном для киберпреступников являются обычные сотрудники. Мы собрали базовые правила информационной безопасности, которые помогут вам защитить бизнес от возможных рисков.

1. Используйте сложные и уникальные пароли

Пароли из простых слов или наборов символов проще подобрать. Требуйте использовать только сложные пароли, состоящие минимум из 12 символов, включая буквы, цифры и спецзнаки.

Плохо: 12345QWERTY

Хорошо: 0wuV8%KneF@L

Запретите записывать пароли на бумаге, сообщать его другим пользователям. При необходимости внедрите в компании менеджер безопасного хранения паролей.

Объясните сотрудникам, почему нельзя использовать один и тот же пароль для всех аккаунтов. Если пароль от одного сервиса будет скомпрометирован, мошенники получат доступ и к другим системам.

2. Подключите двухфакторную аутентификацию

Двухфакторная аутентификация (2FA) — это один из самых эффективных способов защиты аккаунтов. Добавляет дополнительный уровень безопасности, требуя не только пароль, но и код подтверждения из смс или e-mail. Настоятельно рекомендуйте сотрудникам подключить 2FA везде, где это возможно: в соцсетях, мессенджерах, почте, банкинге, маркетплейсах. Это значительно усложнит задачу мошенникам, даже если они узнают пароль.

3. Используйте бизнес-мессенджер для рабочих коммуникаций

Личные мессенджеры — идеальная точка входа для мошенников. Аккаунт сотрудника могут взломать или подделать, и все файлы — и личные, и корпоративные — попадут в руки хакеров. С развитием нейросетей злоумышленники активно применяют социальную инженерию. Например, отправляют жертве от имени коллеги или директора фейковое видео или аудиосообщение с какой-то просьбой.

Чтобы этого избежать, переведите все рабочие коммуникации в защищённый бизнес-мессенджер, где нет случайных людей, спама и отвлекающей информации. К примеру, Битрикс24. Ограничьте возможность использовать личные мессенджеры и соцсети с рабочих устройств.

4. Регулярно обновляйте софт

Устаревшее программное обеспечение — уязвимость, которую могут использовать мошенники. Убедитесь, что все корпоративные устройства и системы регулярно обновляются. Это касается операционных систем, антивирусов, офисных приложений и других программ. Настройте автообновление ПО или назначьте ответственного за контроль обновлений.

5. Установите надёжный антивирус

Современные антивирусные решения обеспечивают комплексную защиту от вредоносных программ, включая трояны, шпионское ПО и руткиты, которые могут похищать учётные данные или отслеживать активность пользователя.

6. Регулярно обучайте кибербезопасности

Человеческий фактор — одна из главных причин утечек данных. Объясните команде, что такое фишинг, и как распознавать фишинговые письма. Для удобства используйте короткую памятку защиты от фишинга, которую мы подготовили в конце чек-листа. Расскажите, что делать при подозрительных запросах и звонках. Организуйте ежеквартальные тренинги и тестовые фишинговые атаки. Проводите работу над ошибками с теми, кто клюнул на удочку хакеров.

7. Назначьте ответственного по вопросам безопасности

Это может быть IT-специалист, специалист по безопасности или руководитель отдела. Проинструктируйте команду: сотрудники должны знать, кому сообщать о подозрительных звонках и письмах.

Красные флаги, которые указывают на фишинговое письмо

- Универсальное, неличное обращение: «Дорогой клиент», «Приветствую». Или нетипичное обращение. К примеру, если в компании все обращаются по имени и на «ты», а в письме — на «Вы» и по имени-отчеству, проявите бдительность.
- Письмо создает иллюзию срочности и вызывает тревогу. Например, письмо от «начальника». Свяжитесь с отправителем напрямую через другой канал связи, чтобы подтвердить подлинность запроса.
- Письмо пришло от подразделения или от сотрудника, который прежде с вами не общался, или же в письме есть нехарактерная просьба.
- Адрес почты вызывает подозрения. Например, компания использует адрес name@company.ru, а письмо пришло с name.company@mail.ru. Или в имени сотрудника есть опечатки.
- Отправитель пишет с личной электронной почты вместо рабочей.
- В письме есть опечатки, ошибки или изображения плохого качества.
- К письму прикреплен zip-файл или большое изображение.
- Ссылки встроены в текст или сокращены, либо при наведении на ссылку отображается другой адрес.

Будьте бдительны, и пусть ваша команда и бизнес всегда будут в безопасности!

Битрикс24