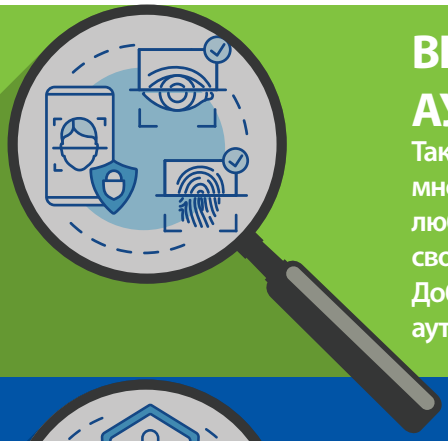
CYBERSECURITY AWARENESS MONTH

УВИДЕТЬ СЕБЯ В КИБЕРПРОСТРАНСТВЕ (SEE YOURSELF IN CYBER)

Каждый играет свою роль в кибербезопасности...независимо от Вашей роли.

Тема кампании «Месяц осведомленности о кибербезопасности 2022 года» — «Увидеть себя в киберпространстве» — демонстрирует, что, хотя кибербезопасность может показаться сложной темой, в конечном счете, на самом деле все дело в людях. Внесите свой вклад в обеспечение кибербезопасности для себя и нашей Компании, выполнив четыре ключевых действия.



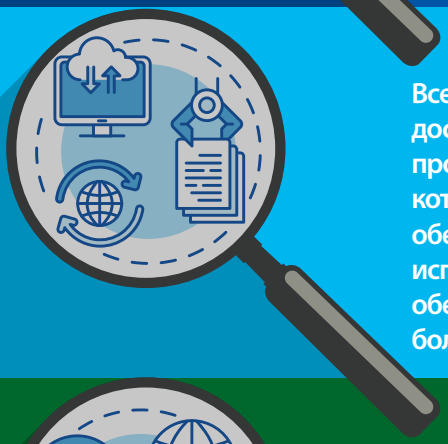
ВКЛЮЧИТЕ МНОГОФАКТОРНУЮ АУТЕНТИФИКАЦИЮ

Также известная как двухфакторная аутентификация и двухэтапная верификация, многофакторная аутентификация – это мера безопасности, которая требует, чтобы любой, кто входит в учетную запись, прошел двухэтапный процесс подтверждения своей личности. Это в два раза затрудняет доступ преступников к онлайн-аккаунту. Добавляя еще один простой шаг при входе в учетную запись, многофакторная аутентификация значительно повышает безопасность Вашей учетной записи.

ИСПОЛЬЗУЙТЕ НАДЕЖНЫЕ ПАРОЛИ

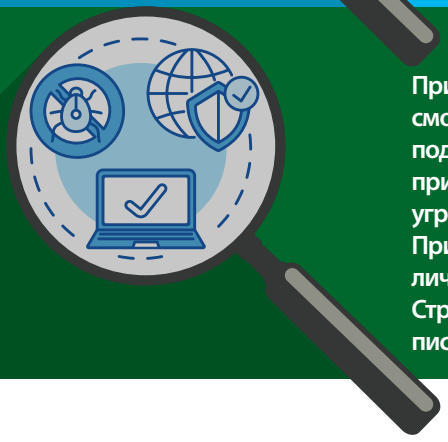
Пароли важны, если Вы хотите сохранить свою информацию в безопасности. Вот несколько простых способов обезопасить свои учетные записи с помощью более эффективных методов использования паролей. Независимо от учетной записи, все пароли должны создаваться с учетом следующих трех концепций:

- Длинный – не менее 12 символов
- Уникальный – для каждой учетной записи нужен свой собственный уникальный пароль
- Сложный – используйте комбинацию прописных и строчных букв, цифр и специальных символов. Некоторые веб-сайты даже позволят Вам использовать пробелы.



ОБЕСПЕЧЕНИЯ

Всегда обновляйте свое программное обеспечение, когда обновления становятся доступными, и не откладывайте их. Данные обновления устраняют общие проблемы с программным обеспечением и предоставляют новые исправления безопасности, в которые могут проникнуть преступники. При загрузке обновления программного обеспечения получайте его только от компании, которая его создала. Никогда не используйте взломанные, пиратские или нелицензионные версии программного обеспечения, поскольку они часто содержат вредоносные программы и вызывают больше проблем, чем решают.



РАСПОЗНАВАЙТЕ ФИШИНГ И СООБЩАЙТЕ О НЕМ

Признаки могут быть незаметными, но как только Вы распознаете попытку фишинга, Вы сможете не попасться на эту удочку. Вот несколько кратких советов о том, как четко определить поддельное фишинговое электронное письмо: Содержит предложение, которое слишком привлекательно, чтобы быть правдой; Язык, который является срочным, тревожным или угрожающим; Плохо написанный текст с орфографическими ошибками и плохой грамматикой; Приветствия, которые являются двусмысленными или очень общими; Просьбы отправить личную информацию; Срочность перехода по незнакомой гиперссылке или вложению; Странные или неожиданные деловые запросы; Адрес электронной почты отправителя в письме не соответствует компании, от которой оно якобы отправлено.

MAUSER
Packaging Solutions