A stack of books with a buckle

Description automatically generated Tệp đã nén

A screenshot of a computer

Description automatically generated Nhập sai mật khẩu

A screenshot of a computer

Description automatically generatedNhập đúng mật khẩu

**Báo cáo: Bảo vệ dữ liệu khi sử dụng các công cụ nén và giải nén**

**1. Thực hành với WinRAR**

* **Nén tập tin/thư mục và thiết lập mật khẩu**:
  1. Chọn tập tin hoặc thư mục cần nén.
  2. Nhấp chuột phải → chọn **Add to archive…**.
  3. Trong cửa sổ WinRAR, nhấn **Set password…**.
  4. Nhập mật khẩu, có thể chọn chế độ **Encrypt file names** để tăng độ bảo mật.
  5. Xác nhận và WinRAR sẽ tạo ra tệp nén có bảo vệ mật khẩu.
* **Giải nén với mật khẩu**:
  1. Nếu nhập **mật khẩu đúng**, WinRAR sẽ giải nén thành công.
  2. Nếu nhập **mật khẩu sai**, quá trình giải nén sẽ thất bại và không thể truy cập nội dung.

**2. Các phương pháp bảo vệ dữ liệu khi nén và giải nén**

* **Đặt mật khẩu bảo vệ tệp nén**: Giúp ngăn chặn truy cập trái phép.
* **Mã hóa tên tệp**: Ẩn thông tin tên file bên trong tệp nén cho đến khi nhập mật khẩu đúng.
* **Chia nhỏ tệp nén**: Giảm rủi ro khi truyền dữ liệu qua mạng, tránh mất toàn bộ dữ liệu nếu một phần bị hỏng.
* **Sử dụng định dạng nén mạnh (RAR, 7z)**: Có hỗ trợ các thuật toán mã hóa tốt hơn.
* **Sao lưu tệp nén bảo mật**: Lưu tại vị trí an toàn (ổ cứng ngoài, USB mã hóa, hoặc dịch vụ lưu trữ đám mây bảo mật).

**3. Tầm quan trọng của bảo mật dữ liệu trong môi trường làm việc**

* **Ngăn ngừa rò rỉ thông tin nhạy cảm**: Dữ liệu doanh nghiệp (tài chính, hợp đồng, thông tin khách hàng) nếu bị lộ có thể gây thiệt hại lớn.
* **Đảm bảo tính toàn vẹn dữ liệu**: Tránh tình trạng bị thay đổi, chỉnh sửa trái phép.
* **Tuân thủ quy định pháp luật và chính sách công ty**: Nhiều tổ chức yêu cầu bảo mật dữ liệu theo tiêu chuẩn (ISO, GDPR, HIPAA...).
* **Tạo sự tin tưởng với khách hàng và đối tác**: Một hệ thống quản lý dữ liệu an toàn sẽ nâng cao uy tín doanh nghiệp.

**4. Cách bảo vệ thông tin nhạy cảm khi dùng WinRAR và các công cụ nén khác**

* Luôn **đặt mật khẩu mạnh** (kết hợp chữ hoa, chữ thường, số, ký tự đặc biệt).
* **Không chia sẻ mật khẩu công khai**; sử dụng kênh bảo mật (mã hóa email, gọi trực tiếp) khi gửi mật khẩu cho người khác.
* **Kích hoạt mã hóa tên file** để ngăn việc lộ thông tin cấu trúc dữ liệu.
* **Sử dụng phiên bản phần mềm chính hãng**, tránh crack để đảm bảo an toàn.
* **Sao lưu dữ liệu** thường xuyên và lưu ở nhiều nơi an toàn.