

Câu 1 ⚡ **Đánh giá Mật khẩu Mẫu**  
Mật khẩu \$77777777\$ được đánh giá là **RẤT YẾU (VERY WEAK)**

Tiêu chí	Đánh giá	Chi tiết
Độ mạnh tổng thể	RẤT YẾU	Dễ dàng bị phá vỡ ngay lập tức bằng các công cụ Brute-force hoặc Dictionary Attack.
Độ dài	8 ký tự	Đủ dài (trên 6), nhưng chưa đủ mạnh (nên từ 12-14 ký tự trở lên).
Độ phức tạp	Rất thấp	Chỉ bao gồm một loại ký tự duy nhất: <b>Số</b> .
Tính ngẫu nhiên	Rất thấp	Mật khẩu là một chuỗi lặp lại của cùng một số.
Thời gian phá vỡ	< 1 giây	Theo các công cụ kiểm tra mật khẩu, một mật khẩu gồm 8 số lặp lại có thể bị phá vỡ gần như ngay lập tức.

Câu 2 : **So sánh các phương pháp đặt mật khẩu**

Dưới đây là một số phương pháp đặt mật khẩu phổ biến để so sánh:

Phương pháp	Ví dụ	Ưu điểm	Nhược điểm	Đánh giá

<b>A. Dựa trên thông tin cá nhân</b>	tendai+ngaysinh	Dễ nhớ.	Cực kỳ dễ đoán nếu thông tin bị lộ trên mạng xã hội.	<b>YẾU</b>
<b>B. Dựa trên từ điển/chuỗi dễ đoán</b>	password123, iloveyou	Dễ nhớ, dễ gõ.	Bị các chương trình tấn công từ điển phá vỡ trong vài giây.	<b>RẤT YẾU</b>
<b>C. Mật khẩu kết hợp (Truyền thống)</b>	M4tkhau!1234	Có đủ các loại ký tự.	Thường bị ngăn, dễ bị tấn công Brute-force nếu hacker biết quy tắc thay thế.	<b>TRUNG BÌNH</b>
<b>D. Mật khẩu dùng cụm từ (Passphrase)</b>	Ca!phe+sua+da!moi+ngay	Dài, phức tạp, dễ nhớ (vì là câu chuyện).	Nếu quá dài và quá phức tạp, có thể khó gõ trên điện thoại.	<b>MẠNH</b>

<b>E. Kết hợp giữa Passphrase &amp; Quy tắc riêng</b>	Cpdm@Fb!2025 (Cà phê đá ngon - Facebook - 2025)	Cực kỳ mạnh vì kết hợp giữa cụm từ và quy tắc tùy chỉnh theo từng trang web.	Cần một công thức nhớ nhất quán.	<b>RẤT MẠNH</b>
---	---	--	----------------------------------	-----------------

### Công thức Mật khẩu Mạnh:

\$\$\text{Công thức Mật Khẩu Mạnh} = \text{Cụm từ Lỗi} + \text{Quy tắc Thay thế} + \text{Mã Trang Web}\$\$

- **1. Cụm từ Lỗi (Passphrase - Dễ nhớ):** Chọn một câu, một cụm từ hoặc bài hát mà bạn thích (ví dụ: "hom nay toi di hoc ve"). Sau đó, thay thế một số chữ cái bằng ký tự đặc biệt/số.
  - Ví dụ: *H0mN@yT0iDIH0cv3* (Thay O \$to\$ 0, A \$to\$ @, I \$to\$ 1, E \$to\$ 3)
- **2. Quy tắc Thay thế (Bảo mật):** Thêm một ký tự đặc biệt cố định ở đầu hoặc cuối.
  - Ví dụ: Thêm dấu chấm than ở cuối: *H0mN@yT0iDIH0cv3!*
- **3. Mã Trang Web (Độc nhất):** Thêm ký hiệu hoặc chữ viết tắt của trang web/tài khoản. Điều này đảm bảo mỗi tài khoản có một mật khẩu duy nhất.
  - Ví dụ cho Gmail: *Gm!*
  - Ví dụ cho Facebook: *Fb\$*

Câu 3 : Thực hành bật 2FA cho email/ mạng xã hội cá nhân, chụp màn hình minh chứng (giấu thông tin nhạy cảm)

Tài khoản của bạn được bảo vệ bằng tính năng Xác minh 2 bước


Hãy ngăn chặn tin tặc truy cập vào tài khoản của bạn bằng một lớp bảo mật nữa.

Nếu không đăng nhập bằng khoá truy cập, bạn sẽ được yêu cầu hoàn tất bước thứ hai an toàn nhất có sẵn trên tài khoản của mình. Bạn có thể cập nhật các bước thứ hai và lựa chọn đăng nhập bất cứ lúc nào trong phần cài đặt. [Chuyển đến phần Cài đặt bảo mật](#)


Tắt Xác minh 2 bước

Bước thứ hai


Hãy đảm bảo bạn có thể truy cập vào Tài khoản Google của mình bằng cách luôn cập nhật thông tin này và thêm các lựa chọn đăng nhập khác



Khoá truy cập và khoá bảo mật

 Thêm khoá bảo mật


>



Lời nhắc của Google

2 thiết bị

>

 **Checklist Quy Tắc Bảo Mật Tài Khoản (Do Sinh viên xây dựng)**

**I. Quy Tắc Về Mật Khẩu (Password Hygiene)**

STT	Quy Tắc	Mô tả / Chi tiết thực hiện
1.	Độ dài tối thiểu	Mật khẩu phải có độ dài tối thiểu là <b>12 - 14 ký tự</b> .

2.	<b>Độ phức tạp</b>	Mật khẩu phải kết hợp đủ 4 loại ký tự (gồm 3 trong 4 là mức tối thiểu): <b>Chữ hoa (A-Z)</b> , <b>Chữ thường (a-z)</b> , <b>Số (0-9)</b> , <b>Ký tự đặc biệt (!@#\$...)</b> .
3.	<b>Tính ngẫu nhiên (Tránh dễ đoán)</b>	Không sử dụng các thông tin cá nhân dễ đoán như tên, ngày sinh, tên thú cưng, hoặc các chuỗi dễ đoán như 123456, qwerty.
4.	<b>Tính độc nhất</b>	<b>Tuyệt đối không sử dụng một mật khẩu cho nhiều tài khoản khác nhau.</b> Nếu một tài khoản bị lộ, tất cả tài khoản còn lại sẽ an toàn.
5.	<b>Công cụ hỗ trợ</b>	Nên sử dụng <b>Trình quản lý mật khẩu (Password Manager)</b> như Google Password Manager, LastPass, 1Password, Bitwarden để lưu trữ và tạo mật khẩu mạnh.

## II. Quy Tắc Công Thức Mật Khẩu Mạnh (Áp dụng từ Nhiệm vụ Cập đôi)

STT	Quy Tắc Công Thức	Công Thức Thực Hiện
6.	<b>Sử dụng Passphrase</b>	Tạo mật khẩu dựa trên một cụm từ hoặc câu dài dễ nhớ, sau đó biến đổi thành ký tự phức tạp.
7.	<b>Quy tắc "Mã hóa"</b>	Thêm một phần ký hiệu hoặc chữ viết tắt <b>độc nhất</b> liên quan đến trang web vào mật khẩu để đảm bảo mỗi tài khoản là duy nhất.
<b>Ví dụ áp dụng:</b>	Công thức chung:	$\text{\text{Cụm từ Lỗi (đã biến đổi)}} + \text{\text{Quy tắc cố định}} + \text{\text{Mã Trang Web}}$

## III. Quy Tắc Xác Thực Hai Yếu Tố (2FA/MFA - Nhiệm vụ Nhóm)

STT	Quy Tắc	Mô tả / Chi tiết thực hiện
8.	<b>Ưu tiên bật 2FA/MFA</b>	Bật <b>Xác thực Hai yếu tố (2FA)</b> hoặc <b>Xác thực Đa yếu tố (MFA)</b> cho <b>tất cả</b> các tài khoản quan trọng (Email chính, Mạng xã hội, Ngân hàng, Lưu trữ đám mây).
9.	<b>Ưu tiên phương pháp 2FA mạnh</b>	Ưu tiên sử dụng <b>Ứng dụng xác thực</b> (như Google Authenticator, Microsoft Authenticator) hoặc <b>Khóa bảo mật vật lý</b> thay vì SMS/Tin nhắn văn bản (vì tin nhắn có thể bị đánh cắp/chuyển hướng).
10.	<b>Lưu trữ mã dự phòng</b>	Lưu trữ các <b>mã khôi phục (backup codes)</b> ở nơi an toàn, ngoại tuyến (ví dụ: viết ra giấy, cất trong két) để dùng khi mất điện thoại.

#### IV. Quy Tắc An Toàn Chung

STT	Quy Tắc	Mô tả / Chi tiết thực hiện
11.	<b>Cảnh giác với Lừa đảo (Phishing)</b>	Luôn kiểm tra kỹ <b>địa chỉ URL</b> và <b>người gửi email/tin nhắn</b> trước khi bấm vào bất kỳ đường link nào hoặc cung cấp thông tin đăng nhập.
12.	<b>Sử dụng kết nối an toàn</b>	Không nên đăng nhập vào các tài khoản quan trọng khi đang sử dụng <b>Wi-Fi công cộng không bảo mật</b> .
13.	<b>Kiểm tra định kỳ</b>	Sử dụng các công cụ kiểm tra rò rỉ dữ liệu (như Have I Been Pwned) để kiểm tra định kỳ xem email/mật khẩu của mình có bị lộ không.