

BẢO VỆ MẬT KHẨU TRƯỚC ĐẠO CHÍCH

Một mật

Một mật khẩu chắc chắn sẽ giúp chống lại sự xâm phạm thông tin, giả danh và rút tiền từ tài khoản của bạn bởi những hacker và những tên trộm cố ý. Vài thủ thuật sau sẽ giúp bạn cải thiện sự bảo mật của máy tính.

Các mật khẩu như thế nào được coi là chắc chắn?

Một mật khẩu chắc chắn và tốt nên gồm 3 tiêu chuẩn sau:

1. Có chiều dài trên 8 kí tự. Những mật khẩu ngắn dễ bị crack (dò ra) hơn những mật khẩu dài.
2. Bao gồm chữ, số và những kí tự như:
 - Không được liên tục hoặc lặp lại hoặc những chữ cái liền kề nhau trên bàn phím. Ví dụ như '12345678', '222222', 'abcdefg'.
 - Không có những từ chung với những chữ cái được thay thế bởi những số hoặc kí tự như là 'M1cr0\$0ft' or 'P@ssw0rd'. Thật không may, những hacker cũng biết những thủ thuật này.
 - Dễ dàng để bạn có thể nhớ được, nhưng khó khăn đối với người khác và:

Không giống tên truy nhập, tên vợ hoặc chồng bạn hoặc ngày sinh của bạn.

Không tìm thấy trong từ điển, ở bất kì ngôn ngữ nào. Những hacker sử dụng những công cụ tinh vi mà có thể nhanh chóng đoán được mật khẩu được sử dụng từ những cơ sở trong từ điển ở những ngôn ngữ khác nhau.

Không khó để nhớ. Những sự kết hợp ngẫu nhiên của những chữ cái, số và kí tự phải được viết dễ nhớ với chính mình.

Tạo mật khẩu chắc chắn theo 4 bước

1. Nghĩ đó là một câu mà bạn có thể nhớ được như là 'Con trai tôi sinh năm 2000'. Đó là một cụm từ dễ nhớ đối với bạn.
2. Lấy chữ cái đầu tiên của mỗi từ của câu để tạo một từ mới. Sử dụng ví dụ trên bạn sẽ nhận được: 'cttsn2'.
3. Chắc chắn hơn bằng cách hãy trộn lẫn chúng bằng việc sử dụng một kiểu kết hợp của những kí tự viết hoa và thường cùng kí tự số. Ví dụ: 'CtTsN2'.
4. Kết thúc, bạn có thể thay thế những kí tự đặc biệt giống như chữ cái, để làm cho mật khẩu trở nên chắc chắn hơn. Ví dụ a->@, o->0, s->\$.

Giữ mật khẩu bí mật

1. Không đưa chúng cho bạn bè hoặc những thành viên trong gia đình (đặc biệt là trẻ nhỏ), những người có thể đưa mật khẩu cho những cá nhân thiếu tin cậy khác.
2. Không được ghi lại những mật khẩu trên bàn làm việc. Nếu bị phát hiện, người khác sẽ dễ dàng truy cập vào máy tính của bạn để ăn trộm.
3. Không bao giờ cung cấp mật khẩu của bạn trên email, thậm chí nếu một công ty hoặc cá nhân có thật yêu cầu nó. Những kẻ lừa đảo "phishing" có thể sử dụng một email lừa đảo để dụ dỗ bạn lộ ra tên sử dụng và mật khẩu và kẻ tội phạm có thể truy cập vào tài khoản của bạn, ăn trộm nhận dạng của bạn và nhiều thứ khác.
4. Thay đổi mật khẩu đều đặn. Lý tưởng nhất là bạn nên tạo mới những mật khẩu chắc chắn cho bạn mỗi tháng.
5. Không sử dụng cùng một mật khẩu cho nhiều tài khoản khác nhau. Bạn nên tạo một mật khẩu mới, chắc chắn mỗi khi bạn mở một tài khoản mới.
6. Đừng bao giờ kích hoạt chế độ nhớ mật khẩu (Save Password).

Phan Anh Chuyên