**Bài 1**

# 1. Nền tảng dữ liệu số là gì?

Nền tảng dữ liệu số là hệ thống tập trung giúp thu thập, lưu trữ và phân tích dữ liệu từ nhiều nguồn. Vai trò của nó là tạo ra một "nguồn sự thật duy nhất", giúp doanh nghiệp quản lý và vận hành hiệu quả hơn.

# 2. Các nguồn dữ liệu phổ biến

Dưới đây là 5 nguồn dữ liệu mà một doanh nghiệp có thể thu thập, cùng với ý nghĩa và cách sử dụng thực tế của chúng:

* **Dữ liệu bán hàng:** Ghi lại giao dịch, sản phẩm bán chạy, giúp đánh giá hiệu suất kinh doanh.
* **Dữ liệu khách hàng:** Thông tin về sở thích, hành vi, giúp cá nhân hóa trải nghiệm và tiếp thị hiệu quả.
* **Dữ liệu marketing và mạng xã hội:** Theo dõi hiệu quả quảng cáo và lắng nghe ý kiến khách hàng.
* **Dữ liệu tài chính:** Báo cáo lợi nhuận, chi phí, giúp theo dõi sức khỏe tài chính doanh nghiệp.
* **Dữ liệu vận hành:** Thông tin sản xuất, chuỗi cung ứng, giúp tối ưu hóa quy trình và giảm lãng phí.

# 3. Lợi ích của việc thống nhất dữ liệu

Thống nhất dữ liệu từ nhiều nguồn mang lại bức tranh toàn cảnh cho doanh nghiệp, giúp ra quyết định nhanh và chính xác hơn. Nó còn tăng cường sự phối hợp giữa các phòng ban, giảm rủi ro và tạo lợi thế cạnh tranh bằng cách phát hiện các xu hướng mới..

**Bài 2**

# 1. Dịch vụ lưu trữ đám mây là gì?

Dịch vụ lưu trữ đám mây là một mô hình cho phép người dùng lưu trữ dữ liệu trên các máy chủ từ xa, thay vì trên thiết bị cá nhân. Lợi ích của nó là bạn có thể truy cập dữ liệu mọi lúc, mọi nơi, trên bất kỳ thiết bị nào có kết nối Internet. Ngoài ra, việc sao lưu và chia sẻ dữ liệu cũng trở nên dễ dàng và an toàn hơn.

# 2. So sánh Google Drive, Dropbox và OneDrive:

|  |  |  |  |
| --- | --- | --- | --- |
| Tiêu chí | Google Drive | Dropbox | OneDrive |
| Dung lượng miễn phí | 15GB | 2GB | 5GB |
| Điểm mạnh | Tích hợp sâu với hệ sinh thái Google (Gmail, Docs, Sheets) | Tốc độ đồng bộ nhanh, giao diện đơn giản, dễ sử dụng | Tích hợp hoàn hảo với Microsoft Office và Windows |
| Đối tượng phù hợp | Người dùng cá nhân, sinh viên, doanh nghiệp sử dụng Google Workspace | Các nhóm làm việc nhỏ, người cần đồng bộ file nhanh chóng | Người dùng Windows và Microsoft 365 |
| Chi phí nâng cấp | Rẻ và linh hoạt với các gói Google One | Các gói cơ bản đắt hơn so với các đối thủ | Có nhiều gói đa dạng, tích hợp với Office 365 |
| Khả năng tích hợp | Mạnh mẽ với các công cụ của Google và nhiều ứng dụng bên thứ ba | Hỗ trợ nhiều ứng dụng và nền tảng | Tốt nhất với các sản phẩm của Microsoft |

**Bài 3**

# 1. Thế nào là mật khẩu mạnh?

Mật khẩu mạnh là mật khẩu có tính ngẫu nhiên cao, khó đoán và khó bị bẻ khóa bởi các công cụ tự động. Một mật khẩu mạnh thường có độ dài tối thiểu 8 ký tự, bao gồm sự kết hợp của chữ cái in hoa, chữ thường, số và ký tự đặc biệt.

# 2. Phân loại và giải thích

| **Mật khẩu** | **Phân loại** |  | **Giải thích** |
| --- | --- | --- | --- |
| **123456** | Yếu |  | Là một dãy số quá đơn giản, dễ đoán và nằm trong danh sách các mật khẩu phổ biến nhất. |
| **ngaysinh2002** | Yếu |  | Dễ đoán vì là thông tin cá nhân và không có sự kết hợp của các loại ký tự khác. |
| **H0c$1nhG!0i** | Mạnh |  | Khó đoán vì có độ dài hợp lý, bao gồm chữ in hoa, số và ký tự đặc biệt thay thế cho chữ cái. |
| **password** | Yếu |  | Là từ khóa rất phổ biến và dễ bị các công cụ bẻ khóa dò tìm. |

# 3. Nguyên tắc tạo mật khẩu an toàn

Để tạo mật khẩu an toàn, bạn nên tuân theo 3 nguyên tắc sau:

1. **Độ dài:** Mật khẩu phải có độ dài tối thiểu từ 8-12 ký tự trở lên.
2. **Sự phức tạp:** Mật khẩu nên kết hợp ngẫu nhiên giữa chữ in hoa, chữ thường, số và ký tự đặc biệt.
3. **Tính duy nhất:** Không sử dụng cùng một mật khẩu cho nhiều tài khoản khác nhau để tránh rủi ro khi một tài khoản bị lộ.

**Bài 4**

# 1. Cách tạo mật khẩu vừa mạnh vừa dễ nhớ

Để tạo một mật khẩu mạnh và dễ nhớ, tôi sẽ dựa trên một câu nói quen thuộc và biến đổi nó bằng cách thay thế các chữ cái thành số hoặc ký tự đặc biệt.

Ví dụ, tôi sẽ chọn câu: **"An toàn thông tin là trên hết, tôi sẽ bảo vệ mật khẩu của mình."**

Sau đó, tôi sẽ thực hiện các bước biến đổi sau:

* **Viết tắt:** "An toàn thông tin" thành "ATTT" và "tôi sẽ bảo vệ" thành "tsbv".
* **Thay thế:** Thay chữ cái "a" bằng "@", "o" bằng "0", "i" bằng "!", "e" bằng "3".
* **Thêm số và ký tự đặc biệt:** Thêm ngày sinh hoặc một số ngẫu nhiên vào cuối.

# 2. Hai ví dụ mật khẩu

1. **Mật khẩu:** ATTT-tsbv-mkcu@309

* **Giải thích:** Mật khẩu này đủ mạnh với độ dài 16 ký tự. Nó bao gồm chữ hoa, chữ thường, số, và ký tự đặc biệt. Mật khẩu dễ nhớ vì được hình thành từ câu nói quen thuộc, giúp bạn dễ dàng gõ lại mà không cần phải ghi nhớ một chuỗi ký tự ngẫu nhiên.

1. **Mật khẩu:** AnToan#thongtin123

* **Giải thích:** Mật khẩu này có độ dài 18 ký tự và bao gồm chữ hoa, chữ thường, số, và ký tự đặc biệt. Mặc dù dựa trên một cụm từ đơn giản, việc thêm ký tự đặc biệt và số ngẫu nhiên vào cuối giúp nó khó bị bẻ khóa hơn rất nhiều so với những mật khẩu thông thường.

**Bài 5**

# 1. Các website an toàn:

* **https://www.vietcombank.com.vn**
  + **Lý do an toàn 1:** Địa chỉ bắt đầu bằng https://, cho thấy website này sử dụng chứng chỉ bảo mật SSL/TLS. Chứng chỉ này mã hóa dữ liệu giữa trình duyệt của bạn và máy chủ, giúp bảo vệ thông tin cá nhân (như tài khoản, mật khẩu) khỏi bị đánh cắp.
  + **Lý do an toàn 2:** Tên miền chính xác là .vietcombank.com.vn, đây là tên miền chính thức của ngân hàng.
* **https://facebook.com**
  + **Lý do an toàn 1:** Website sử dụng giao thức https:// và có biểu tượng ổ khóa trên thanh địa chỉ, xác nhận rằng kết nối của bạn được bảo mật.
  + **Lý do an toàn 2:** Tên miền chính xác là .facebook.com, là tên miền chính thức và được công nhận rộng rãi.

# 2. Các website không an toàn:

* **http://secure-vietcombank-login.com**
  + **Lý do không an toàn 1:** Địa chỉ bắt đầu bằng http:// (không có chữ 's'), nghĩa là dữ liệu không được mã hóa. Bất kỳ thông tin nào bạn nhập vào trang web này đều có thể bị đọc trộm bởi tin tặc.
  + **Lý do không an toàn 2:** Tên miền không chính xác. Mặc dù có các từ khóa liên quan đến "Vietcombank" và "login", đây là một trang web giả mạo (lừa đảo phishing) được tạo ra để đánh lừa người dùng nhập thông tin đăng nhập.
* **http://free-gift-now.info**
  + **Lý do không an toàn 1:** Website không sử dụng https:// và không có chứng chỉ bảo mật, khiến mọi thông tin nhập vào đều có nguy cơ bị lộ.
  + **Lý do không an toàn 2:** Tên miền nghe có vẻ hấp dẫn và không chuyên nghiệp, thường là dấu hiệu của các trang web lừa đảo hoặc chứa mã độc. Những trang web này thường yêu cầu bạn cung cấp thông tin cá nhân để nhận quà tặng hoặc ưu đãi giả.

**Bài 6**

# 1. Phân tích các thông tin nhạy cảm đã bị lộ

Với nội dung bài đăng trên Facebook, bạn đã vô tình tiết lộ một lượng lớn thông tin nhạy cảm, bao gồm:

* **Ngày sinh:** 08/09/2002.
* **Địa chỉ nhà:** Số nhà 123, đường Lê Lợi.
* **Sự vắng mặt:** Thông tin về sinh nhật có thể ngụ ý rằng bạn sẽ không có mặt ở nhà.

# 2. Cách tin tặc có thể lợi dụng

* **Tấn công lừa đảo (Phishing):** Tin tặc có thể sử dụng ngày sinh và tên đường phố để tạo các email hoặc tin nhắn lừa đảo. Ví dụ, họ có thể gửi một email giả mạo ngân hàng với tiêu đề "Chúc mừng sinh nhật" và yêu cầu bạn cập nhật thông tin để chiếm đoạt tài khoản.
* **Lừa đảo chiếm đoạt tài khoản:** Kết hợp ngày sinh, địa chỉ nhà với các thông tin công khai khác trên mạng xã hội, tin tặc có thể đoán được mật khẩu, câu hỏi bảo mật, hoặc thậm chí là mã PIN ngân hàng, từ đó chiếm đoạt tài khoản trực tuyến của bạn.
* **Trộm cắp vật lý:** Địa chỉ nhà công khai có thể khiến bạn trở thành mục tiêu của những kẻ trộm cắp, đặc biệt là khi chúng biết rằng bạn sẽ vắng mặt để đi dự tiệc sinh nhật.

# 3. Ba cách bảo mật thông tin cá nhân trên mạng xã hội

Để bảo vệ thông tin cá nhân, bạn nên tuân thủ các nguyên tắc sau:

1. **Thiết lập quyền riêng tư:** Luôn cài đặt chế độ riêng tư cho bài đăng của bạn, chỉ chia sẻ với bạn bè hoặc những người bạn tin tưởng. Tránh để thông tin như ngày sinh, địa chỉ, hoặc số điện thoại ở chế độ công khai.
2. **Hạn chế chia sẻ thông tin nhạy cảm:** Tránh đăng tải các thông tin chi tiết về cá nhân như địa chỉ, số điện thoại, ngày tháng năm sinh hoặc lịch trình di chuyển. Kể cả khi đi du lịch, bạn nên đợi đến khi trở về nhà rồi mới đăng ảnh.
3. **Cẩn trọng với các bài đăng chung:** Đừng chia sẻ bài đăng từ các ứng dụng hoặc trò chơi yêu cầu quyền truy cập vào thông tin cá nhân của bạn. Những ứng dụng này có thể thu thập dữ liệu và bán lại cho bên thứ ba hoặc bị tin tặc tấn công.

**Bài 7**

# 1. Cách kiểm tra mà không nhấn trực tiếp

Để kiểm tra đường link rút gọn mà không bấm vào, bạn có thể sử dụng các công cụ trực tuyến chuyên dụng. Những công cụ này sẽ giúp bạn xem địa chỉ đích cuối cùng của link mà không cần phải truy cập.

#### 2. Các công cụ và cách thức kiểm tra

* **Sử dụng công cụ mở rộng link (URL Expander):** Các trang web như **CheckShortURL** hoặc **URL Expander** cho phép bạn dán link rút gọn vào, và chúng sẽ hiển thị URL gốc cùng với một số thông tin khác như tiêu đề trang, loại mã độc (nếu có).
* **Thử gõ thủ công:** Một số dịch vụ rút gọn link cho phép bạn xem trước bằng cách thêm dấu + vào cuối đường link. Ví dụ: nhập https://bit.ly/3xyzABC+ vào thanh địa chỉ.
* **Sử dụng các dịch vụ quét mã độc:** Các dịch vụ như **VirusTotal** hoặc **Google Transparency Report** có thể phân tích đường link và kiểm tra xem nó có nằm trong danh sách các trang web lừa đảo (phishing) hoặc chứa mã độc hay không.

# 3. Tại sao link rút gọn thường được dùng trong lừa đảo?

Link rút gọn là công cụ phổ biến cho lừa đảo (phishing) vì một số lý do:

* **Che giấu địa chỉ gốc:** Kẻ tấn công có thể ẩn một địa chỉ trang web lừa đảo hoặc chứa mã độc đằng sau một đường link rút gọn trông vô hại và uy tín.
* **Tạo cảm giác an toàn:** Một đường link rút gọn trông ngắn gọn, sạch sẽ và thường khiến người dùng mất cảnh giác, dễ dàng bấm vào mà không kiểm tra.

**Bài 8**

# 1. Phân loại các phần mềm độc hại

* **Virus / Trojan:** Khi máy tính chạy chậm bất thường và quạt kêu to, có khả năng cao máy đã bị nhiễm virus hoặc trojan. Các phần mềm này thường chiếm dụng tài nguyên CPU, bộ nhớ, hoặc băng thông mạng để thực hiện các tác vụ ngầm như khai thác tiền ảo, gửi spam, hoặc tấn công máy tính khác.
* **Adware:** Hiện tượng xuất hiện nhiều cửa sổ quảng cáo lạ và trình duyệt tự động mở tab khi khởi động là dấu hiệu của adware. Đây là loại phần mềm độc hại được thiết kế để hiển thị quảng cáo không mong muốn nhằm tạo ra doanh thu cho kẻ tấn công.
* **Ransomware:** Các file trong máy bị đổi tên sang đuôi .locked là dấu hiệu rõ ràng nhất của ransomware. Phần mềm này mã hóa dữ liệu của người dùng và đòi tiền chuộc để khôi phục lại.

# 2. Cách xử lý ngay khi phát hiện

Khi phát hiện các dấu hiệu trên, bạn cần hành động ngay lập tức để giảm thiểu thiệt hại:

1. **Ngắt kết nối mạng:** Ngay lập tức ngắt kết nối Internet (rút dây mạng hoặc tắt Wi-Fi) để ngăn chặn malware lây lan và truyền dữ liệu ra ngoài.
2. **Khởi động lại ở chế độ an toàn (Safe Mode):** Chế độ này chỉ cho phép các chương trình cần thiết của hệ điều hành chạy, giúp vô hiệu hóa hầu hết các phần mềm độc hại.
3. **Quét virus toàn diện:** Sử dụng một phần mềm diệt virus uy tín (như Malwarebytes, Avast hoặc Kaspersky) để quét toàn bộ hệ thống và xóa các file độc hại.
4. **Sao lưu dữ liệu:** Nếu có thể, hãy sao lưu các dữ liệu quan trọng ra ổ cứng ngoài hoặc dịch vụ lưu trữ đám mây.

**Bài 9**

# 1. Định nghĩa

**Phần mềm bản quyền** là phần mềm được mua hợp pháp từ nhà phát triển, người dùng có giấy phép sử dụng đầy đủ. Ngược lại, **phần mềm lậu** là phiên bản bất hợp pháp, được sao chép, bẻ khóa hoặc phân phối mà không có sự cho phép của tác giả.

# 2. Lợi ích khi dùng phần mềm bản quyền

* **Bảo mật và an toàn:** Phần mềm bản quyền thường xuyên được cập nhật các bản vá lỗi và lỗ hổng bảo mật, giúp bảo vệ máy tính của bạn khỏi virus và các cuộc tấn công mạng.
* **Hỗ trợ kỹ thuật chính hãng:** Khi gặp vấn đề, bạn sẽ nhận được sự hỗ trợ trực tiếp từ nhà phát triển, giúp giải quyết các lỗi một cách nhanh chóng.
* **Đầy đủ tính năng và cập nhật:** Bạn được quyền sử dụng toàn bộ các tính năng mới nhất và nhận được các bản cập nhật định kỳ để cải thiện hiệu suất.

# 3. Rủi ro khi dùng phần mềm lậu

* **Nguy cơ mất an toàn:** Phần mềm lậu thường đi kèm với mã độc, virus hoặc các phần mềm gián điệp, có thể đánh cắp thông tin cá nhân và làm hỏng hệ thống của bạn.
* **Vi phạm pháp luật:** Sử dụng phần mềm lậu là hành vi vi phạm bản quyền, có thể dẫn đến các hậu quả pháp lý nghiêm trọng như phạt hành chính hoặc truy tố.
* **Thiếu ổn định và tính năng:** Các phiên bản lậu thường không ổn định, dễ gặp lỗi và không thể nhận được các bản cập nhật quan trọng, khiến trải nghiệm sử dụng không tốt.

**Bài 10**

# 1. Định nghĩa

Xác thực hai lớp (2FA) là một lớp bảo mật bổ sung cho tài khoản trực tuyến của bạn. Khi bạn đăng nhập, ngoài việc nhập mật khẩu, bạn sẽ cần cung cấp thêm một mã xác minh từ một thiết bị hoặc ứng dụng khác, chẳng hạn như điện thoại di động.

# 2. Ba lợi ích khi bật 2FA

1. **Bảo vệ tài khoản an toàn hơn:** Ngay cả khi tin tặc lấy được mật khẩu của bạn, chúng vẫn không thể truy cập vào tài khoản vì không có mã xác thực lớp thứ hai.
2. **Ngăn chặn truy cập trái phép:** 2FA giúp phát hiện và ngăn chặn các nỗ lực đăng nhập đáng ngờ từ các thiết bị hoặc địa điểm không xác định.
3. **Bảo vệ dữ liệu cá nhân:** Việc bật 2FA sẽ bảo vệ email, tin nhắn và các thông tin nhạy cảm khác khỏi bị lộ khi tài khoản của bạn bị xâm nhập.

# 3. Các bước bật 2FA trên Gmail

1. **Truy cập Cài đặt:** Đăng nhập vào tài khoản Gmail, sau đó vào **Quản lý Tài khoản Google** (Manage your Google Account).
2. **Vào mục Bảo mật:** Chọn tab **Bảo mật** (Security) ở menu bên trái.
3. **Kích hoạt:** Cuộn xuống và tìm mục **"Xác minh 2 bước"** (2-Step Verification), sau đó làm theo các hướng dẫn trên màn hình. Bạn sẽ được yêu cầu nhập số điện thoại để nhận mã xác minh qua tin nhắn.