

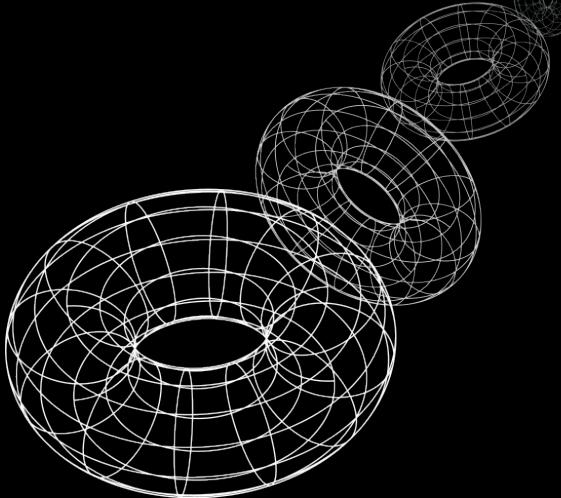
Security Awareness Training

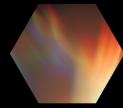
CYBERSECURITY AWARENESS

Tips to protect you and your data

Presented By: Le Hong Hai | Security Engineer

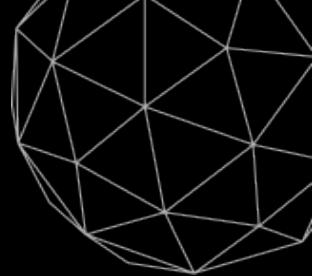
TỔNG QUAN

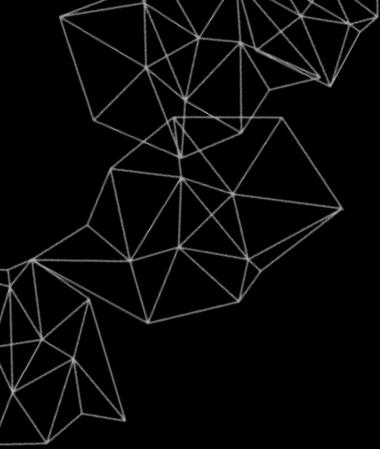




#whoami

- 4+ years of cybersecurity experience
- Malware analysis
- Computer forensics
- Security incident response

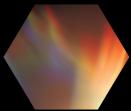




Pham Huu Loc

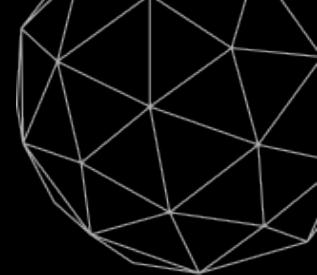


Một số thống kê

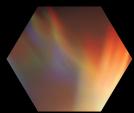


- Báo cáo điều tra vi phạm dữ liệu năm 2021 của **Verizon**: **85%** các cuộc tấn công lớn là nhắm vào người dùng
- Báo cáo Thị trường An toàn thông tin Việt Nam năm 2021 của **Viettel Cyber Security**: Hơn **3000** cuộc tấn công lừa đảo nhắm vào người dùng
- Báo cáo hoạt động của Ransomware năm 2021 của **VirusTotal**: Việt Nam nằm trong **TOP 3** quốc gia bị ảnh hưởng nhiều nhất

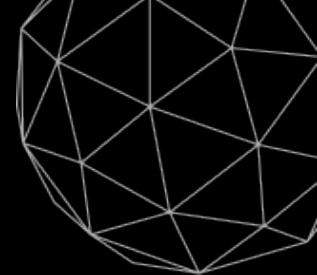




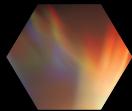
Bài học từ câu chuyện có thật



- Năm 2014: **Sony Pictures** bị hack làm rò rỉ nhiều thông tin bí mật. Sony báo cáo thiệt hại **35** triệu đô
- Năm 2013: Tập đoàn bán lẻ **Target** của Mỹ bị hack, tin tặc đánh cắp hơn 110 triệu số thẻ tín dụng, hồ sơ người tiêu dùng. Thiệt hại được báo cáo là **162** triệu đô
- Năm 2014: **Văn phòng Quản lý Nhân sự Hoa Kỳ (OPM)** bị hack, hơn **20** triệu hồ sơ nhân viên và nhà thầu chính phủ bị xâm phạm



Bài học từ câu chuyện có thật



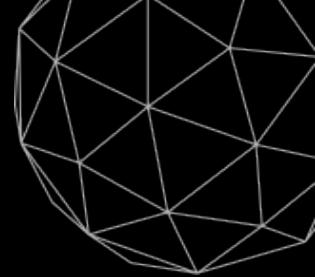
- Năm 2021: **Colonial Pipeline** bị hack khiến công ty này phải đóng cửa đường ống dẫn dầu, tạm dừng vận chuyển xăng dầu đến bờ biển phía đông Hoa Kỳ. Công ty này thừa nhận đã trả cho bọn tội phạm **4.4** triệu đô để đổi lại quyền kiểm soát hệ thống.
- Năm 2022: **Rockstar** bị hack, tin tặc cung cấp nhiều video game và mã nguồn của **GTA 6**
- Năm 2022: **Uber** bị hack làm lộ **57** triệu hồ sơ khách hàng.

Bảo mật giống như
hơi thở. Chúng ta
cần nó

Lau Lau

chà chà





Quan niệm sai lầm

“

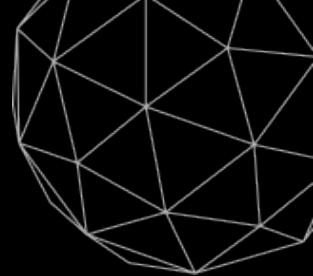
*Tôi chẳng có dữ liệu gì để “hắc-cơ”
hack cả!*



Record Type	Average Price
Health Care Record	\$250.15
Payment Card Details	\$5.40
Banking Records	\$4.12
Access Credentials	\$0.95
Social Security Number	\$0.53
Credit Record	\$0.31
Basic PII	\$0.03

Demographic		Cost for Data Per Person	Percentage of Population
Sex Assignment	Male	\$0.15	48.59%
	Female	\$0.14	51.41%
Age	Age 18-24	\$0.36	11.92%
	Age 55+	\$0.05	32.33%
Ethnicity	Middle Eastern	\$0.62	1.21%
	Hispanic	\$0.01	8.09%
Family Annual Income	\$40,000-\$49,999	\$0.02	4.94%
	\$120,000-\$149,999	\$0.33	1.84%

Tham khảo: <https://www.invisibly.com/learn-blog/how-much-is-data-worth>



Quan niệm sai lầm

“

*Tin tức hack vào các công ty lớn,
chắc nó “chừa” mình ra!*

MỚI NHẤT: Thúc đẩy nghiên cứu ứng dụng mật mã, an toàn thông tin vào chuyển đổi số tại Việt Nam Sau iPhone

BẢO MẬT

Nhiều doanh nghiệp vừa và nhỏ ở Việt Nam bị đánh cắp thông tin khách hàng

Thích 138 Chia sẻ Quan tâm 1

08/10/2021 05:42 GMT+7

Theo một nghiên cứu mới của Cisco, 59% doanh nghiệp vừa và nhỏ tại Việt Nam gặp sự cố mạng trong năm qua. Điều này khiến nhiều thông tin của khách hàng rơi vào tay hacker.

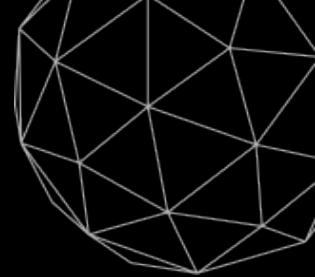
- ▶ **Sự cố tấn công mạng vào các hệ thống tại Việt Nam giảm nhẹ trong tháng 9**
- ▶ **Tấn công mạng vào Việt Nam giảm, nhưng mức độ ngày càng tinh vi**

Cisco vừa công bố kết quả nghiên cứu "An ninh mạng cho các doanh nghiệp vừa và nhỏ tại khu vực Châu Á - Thái Bình Dương chuẩn bị phòng thủ số".

Kết quả nghiên cứu, 59% doanh nghiệp vừa và nhỏ tại Việt Nam gặp sự cố mạng trong 12 tháng qua. Các sự cố tấn công mạng đã khiến 86% số doanh nghiệp bị mất thông tin khách hàng vào tay kẻ xâm



<https://ictnews.vietnamnet.vn/bao-mat/nhieu-doanh-nghiep-vua-va-nho-o-viet-nam-bi-danh-cap-thong-tin-khach-hang-394462.html>



Quan niệm sai lầm

“

Bảo mật đã có mấy ông kỹ thuật lo!

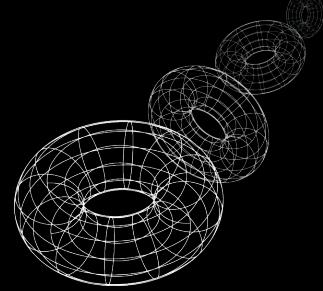
- 
- Defense in Depth
 - Patched systems
 - 24/7 monitoring/ alerting
 - Annual compliance auditing
 - Experienced IT/ Security team



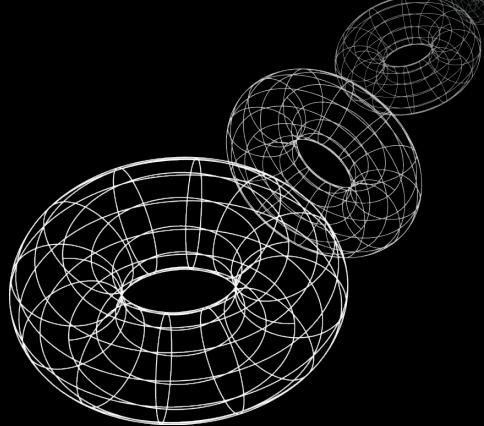
User clicks on
an email

made with mematic

Nội dung

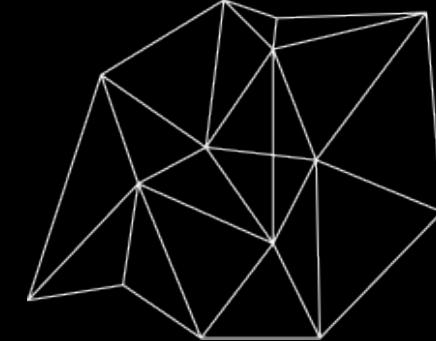


- 1 Tại sao cần nhận thức ATTT
- 2 Sao lưu, sao lưu, sao lưu
- 3 Cập nhật bản vá
- 4 Mật khẩu
- 5 Xác thực hai yếu tố
- 6 An toàn internet & email
- 7 Lừa đảo qua điện thoại
- 8 Quyền riêng tư
- 9 Phải làm gì khi gặp sự cố ATTT
- 10 Q&A



TẠI SAO CẦN NHẬN THỨC ATTT

Tại sao cần nhận thức ATTT



- Chỉ riêng công nghệ **KHÔNG THẺ** bảo vệ bạn
- Tin tặc thường tấn công vào nơi bảo mật yếu nhất
- Mỗi người đều là một mắt xích
- Nhận thức ATTT giúp bạn giảm thiểu rủi ro, sự cố
- Nhận thức về ATTT dành cho...
 - Nhân viên
 - Cha mẹ
 - ...
 - Lãnh đạo
 - Trẻ em
 - Tất cả!



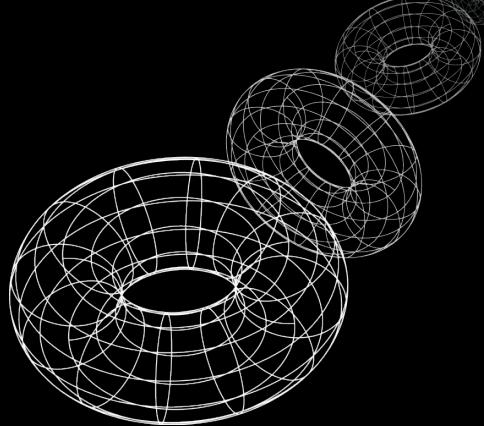
*Những mẹo giúp bạn an toàn tại nơi làm việc cũng sẽ
giúp bạn an toàn khi ở nhà*





COOKIE HÂN HOAN

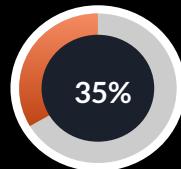




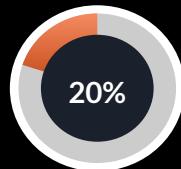
SAO LƯU DỮ LIỆU

Sao lưu dữ liệu

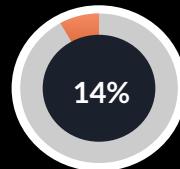
- Bản sao lưu là cứu tinh của bạn khi gặp sự cố
 - Không thể hoàn hảo
 - Bảo vệ chống lại ransomware
- Phương tiện sao lưu **không nên** kết nối liên tục
- Thường xuyên kiểm tra bản sao lưu, thử khôi phục



Người dùng
chưa bao giờ
sao lưu



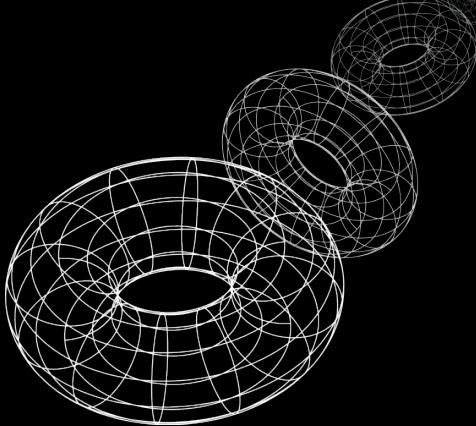
Người dùng
sao lưu hàng
năm



Người dùng
sao lưu hàng
tháng



Người dùng
sao lưu hàng
ngày



CẬP NHẬT BẢN VÁ

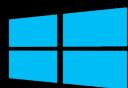
Cập nhật là rất cần thiết

- Những gì an toàn của ngày hôm qua có thể không an toàn hôm nay
- Các lỗ hổng phần mềm được tìm thấy mỗi ngày
- Hơn **360000** mã độc được phát tán mỗi ngày
- **Phần mềm càng cũ càng dễ bị tin tặc tấn công.**

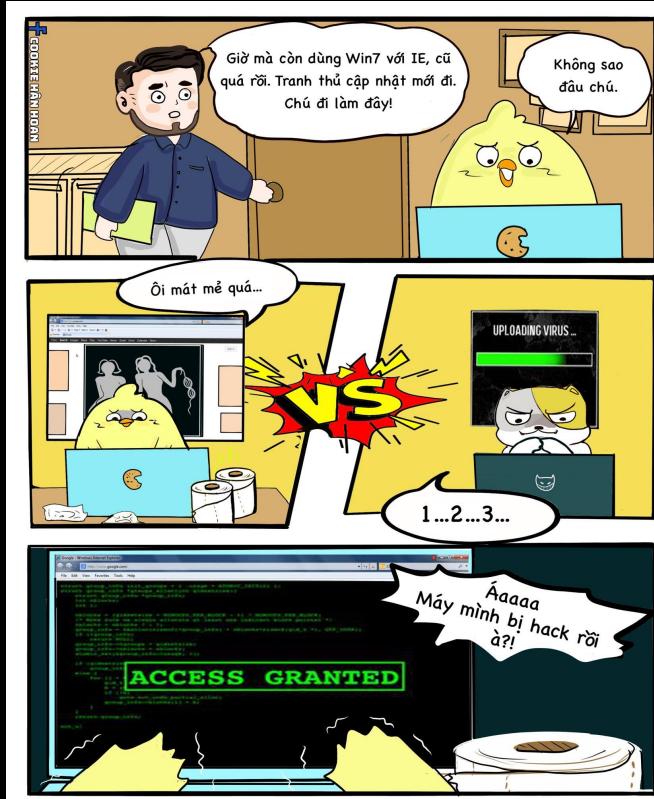


Giữ cho hệ thống luôn được cập nhật

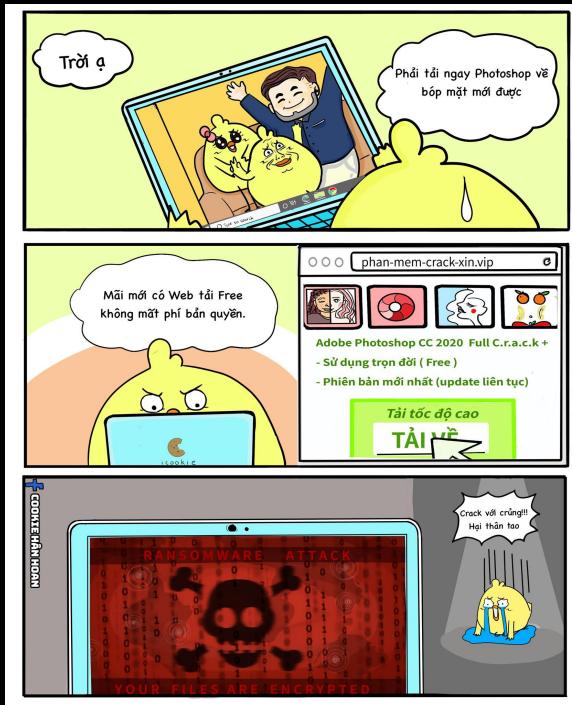
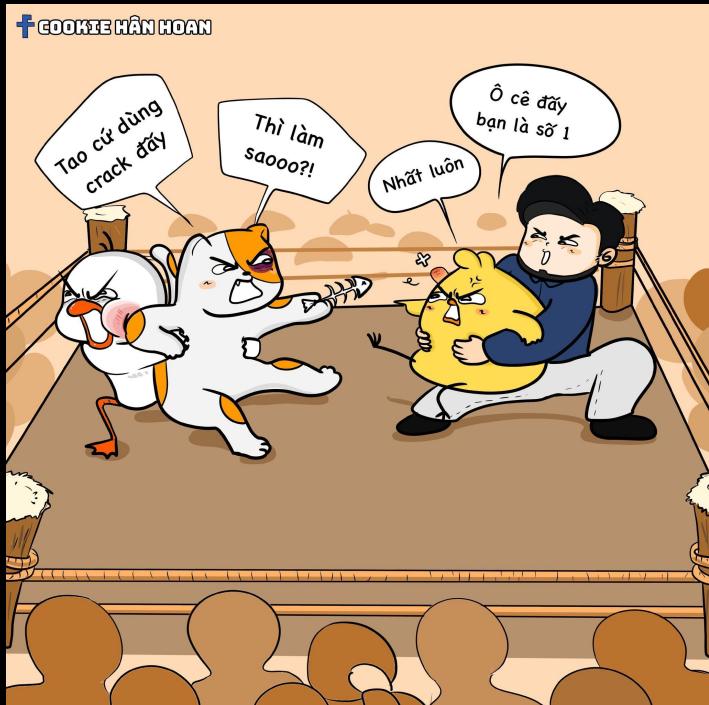
- Hệ điều hành
 - Windows, macOS, Linux
 - ~~Windows 7: EOL 01/2020~~
- Anti-virus
 - Cập nhật các mẫu nhận diện mới nhất để phát hiện được các loại mã độc mới
 - Eset, Kaspersky, Symantec/Norton, McAfee, Windows Defender, Avast, ...



Giữ cho hệ thống luôn được cập nhật



Thói quen xấu khi cài phần mềm



Thói quen xấu khi cài phần mềm



Mua phần mềm diệt virus bản quyền

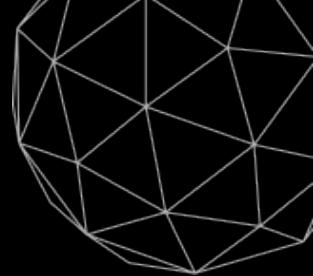


Bật chế độ quét sâu



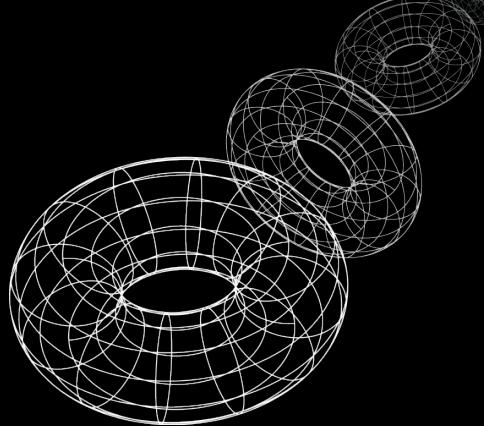
Virus

Đừng quên!!!



- Trình duyệt
 - Chrome, Firefox, Edge, Safari, Brave, etc.
 - ~~Internet Explorer~~
- Thiết bị di động
- Các thiết bị IoT
- **Thực hiện việc này thường xuyên**





MẬT KHẨU

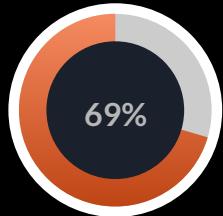
Quản lý mật khẩu

- Giữ mật khẩu ở một vị trí an toàn
 - Không sử dụng giấy note
 - Không lưu mật khẩu dạng rõ trên máy tính
- Trình quản lý mật khẩu (aka vault)
 - Bitwarden
 - KeePass
 - LastPass
 - ~~Chrome?~~
 - ~~Apple Keychain?~~
- Lợi ích của trình quản lý mật khẩu
 - Mật khẩu được lưu trữ ở nơi an toàn
 - Sử dụng một mật khẩu để quản lý
 - Tự động điền username/password trên web
 - Đồng bộ Desktop - Laptop - Mobile

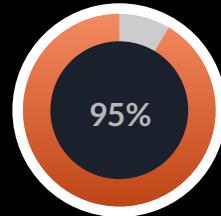


Password Tips

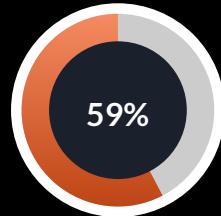
- Tránh sử dụng mật khẩu có liên quan đến
 - Địa chỉ
 - Số điện thoại
 - Tên thú cưng
 - Tên con cái
 - Ngày sinh
 - Thú vui, sở thích
- Mỗi tài khoản một mật khẩu riêng
- Được tạo tự động, gần như không thể đoán được



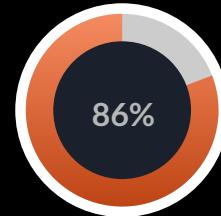
Mật khẩu được chia sẻ với đồng nghiệp



Mật khẩu được chia sẻ với gia đình



Một mật khẩu cho tất cả các tài khoản



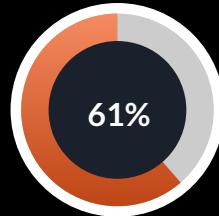
Mật khẩu quá "đơn giản"

Password Tips



Passphrases, not passwords?

- Kết hợp của cụm từ dài nhưng dễ nhớ
- Không dễ bị đoán:
 - Kết hợp của nhiều từ
 - Độ dài ưu tiên hơn độ phức tạp (hơn 12 ký tự)
 - Bad password (8): P@ssw0rd
 - Great password (25): MySonWasBornNovember2345!



Mật khẩu 8 ký tự



Độ dài mật khẩu trung bình



Số chữ thường trung bình



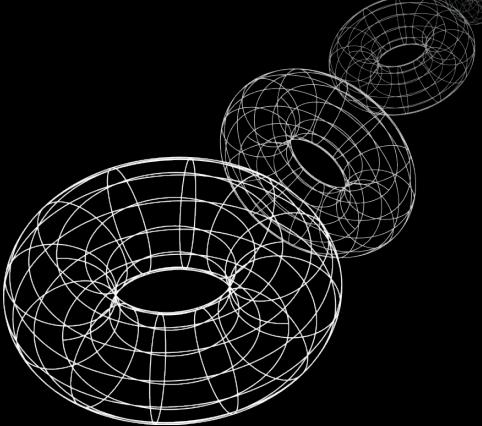
Số ký tự đặc biệt trung bình

Top 20 mật khẩu

Rank	2018	2019	2020	Rank	2018	2019	2020
1	123456	123456	123456	11	princess	abc123	1234567
2	password	123456789	123456789	12	admin	qwerty123	qwerty
3	123456789	qwerty	picture1	13	welcome	1q2w3e4r	abc123
4	12345678	password	password	14	666666	admin	Million2
5	12345	1234567	12345678	15	abc123	qwertyuiop	000000
6	111111	12345678	111111	16	football	654321	1234
7	1234567	12345	123123	17	123123	555555	iLoveYou
8	sunshine	iloveyou	12345	18	monkey	lovely	aaron431
9	qwerty	111111	1234567890	19	654321	7777777	password1
10	iloveyou	123123	senha	20	!@#\$%^&*	welcome	qqww1122

Thay đổi ngay nếu đang sử dụng trong số này

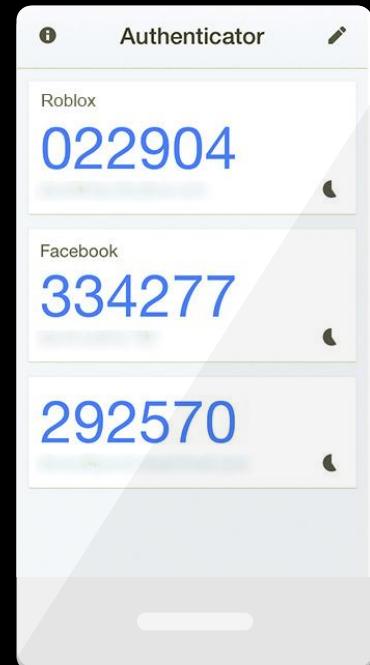
XÁC THỰC HAI YẾU TỐ



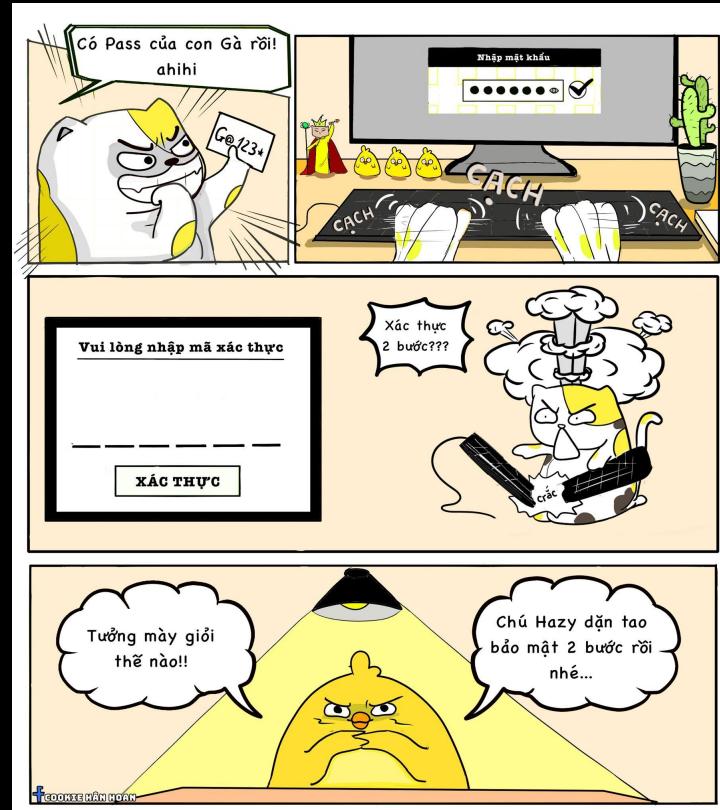
Xác thực hai yếu tố - 2FA

- Thêm bước xác thực ngoài username và password
- Nhận mã xác thực qua:
 - Email
 - Phone pop-up
 - Applications
 - Google Authenticator
 - Authy (*)
 - Phone Call
 - SMS

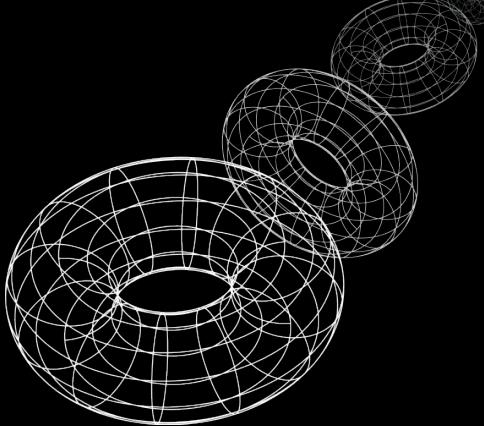
Not as
secure



Xác thực hai yếu tố - 2FA



AN TOÀN INTERNET & EMAIL



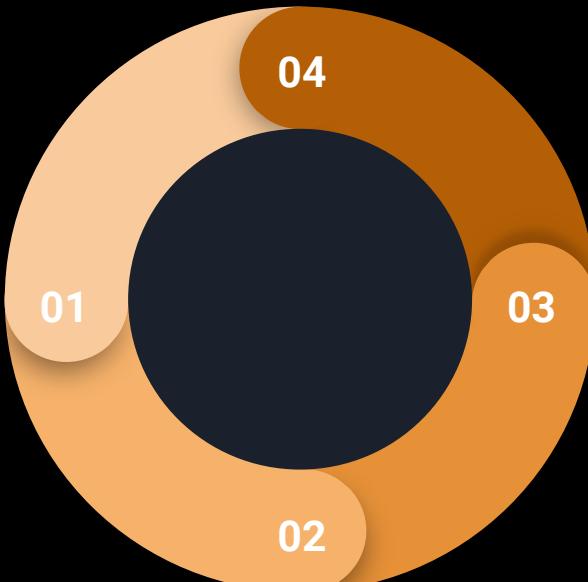
Xác định một đường link có an toàn

B1. Verify

- o Email
- o Mạng xã hội
- o SMS/iMessage
- o Zoom, Teams, Slack
- o etc.

B2. Hover

Di chuột qua đường link để xem chính xác nó dẫn đến đâu



B4. Click

Có vượt qua 3 bài kiểm tra không? Nếu vẫn nghi ngờ tốt nhất không click

B3. Sniff test

Có nhận ra trang web này không?
Nó có quen thuộc không?
Hãy luôn đặt nghi vấn!

Link bị rút gọn hoặc xáo trộn?

- Một số dịch vụ:
 - Bit.ly
 - TinyURL
- Rất phổ biến và tiện dụng
- Hay bị tin tặc lợi dụng để ẩn các trang web độc hại

Link expander
www.linkexpander.com



https://bit.ly/3ydGfNp

Expand

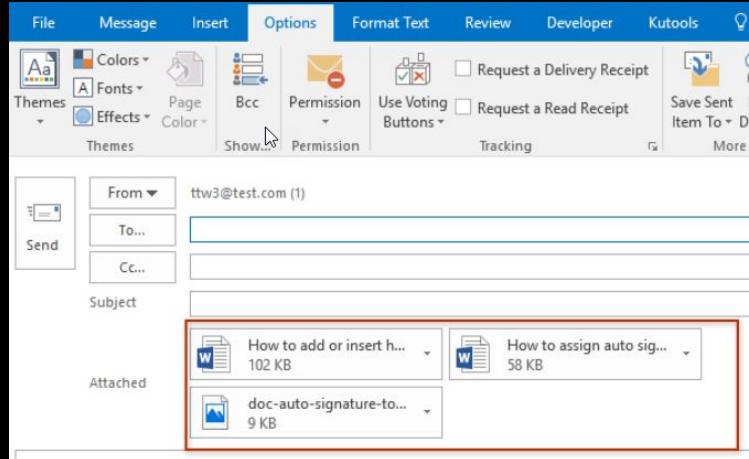
Uncovered URL is:

https://bizflycloud.vn/ve-bizflycloud

Tệp đính kèm email

- Dừng! và suy nghĩ
- Có nhận ra người gửi không?
- Có mong đợi một tệp đính kèm?

Attachments in email client (Microsoft Outlook)



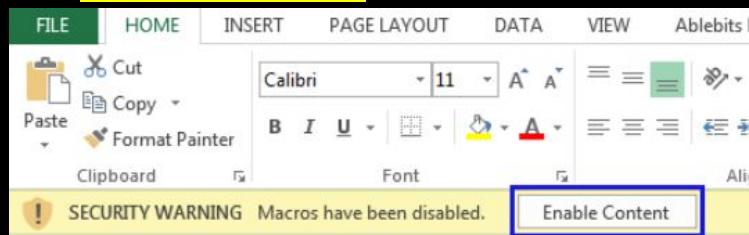
92% phần mềm độc hại gửi qua email

Macros

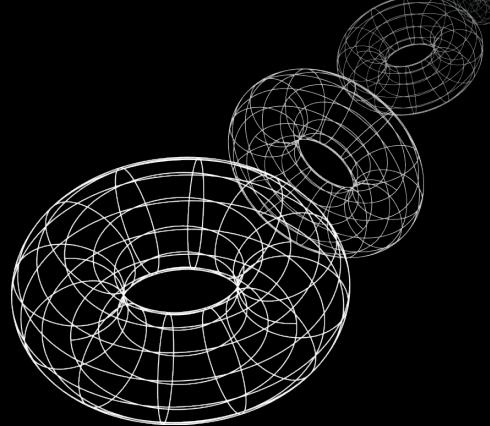


- B1: Không Enable Content
- B2: Xem lại bước 1

Enable Macros <- NOOOOOO!!!!



LỪA ĐẢO QUA ĐIỆN THOẠI

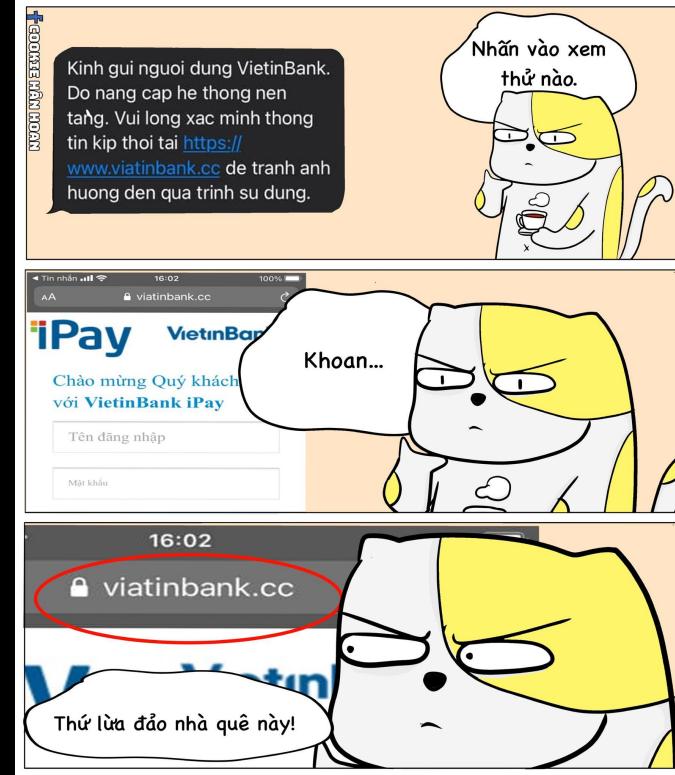


Lừa đảo qua điện thoại

- **Social engineering?**
 - Ngân hàng, tín dụng
 - Y tế, bảo hiểm
 - Mục tiêu: truy cập dữ liệu nhạy cảm
- Số điện thoại dễ bị mạo danh
 - Yêu cầu người gọi cung cấp thông tin
 - Gọi lại xác minh theo số đã công bố
- Dạng phổ biến khác
 - Lừa đảo người già
 - Tech support - Microsoft, Apple, Dell,.. sẽ không bao giờ tự liên hệ với người dùng thường.

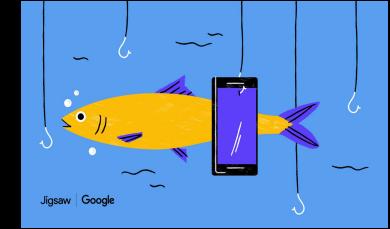


Lừa đảo qua điện thoại



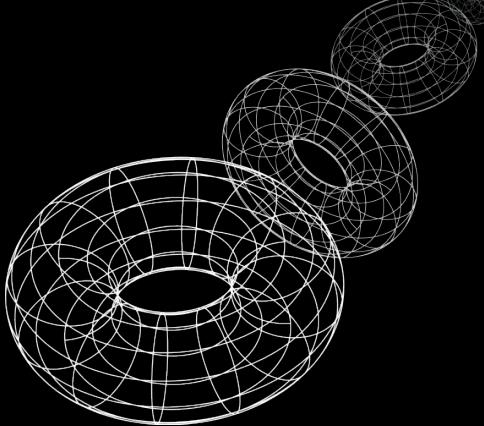
Phishing Quiz

- Phishing Quiz: Jigsaw:
<https://phishingquiz.withgoogle.com/?hl=vi>



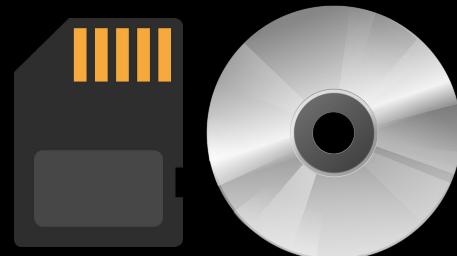
- Dấu Hiệu Lừa Đảo:
<https://www.dauhieuluadao.com/quiz/>

MẸO & QUYỀN RIÊNG TƯ



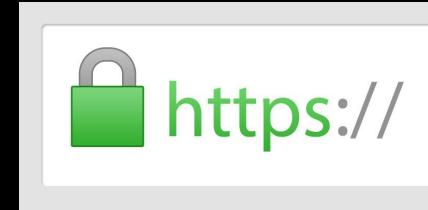
Thiết bị lưu trữ, di động

- Không kết nối các thiết bị lạ, không xác định
- Các chương trình độc hại có thể khởi chạy khi cắm thiết bị mà ko cần bạn làm gì cả
- Ví dụ:
 - USB/flash drives
 - Thẻ SD, micro SD
 - Đĩa CDs/DVDs
 - Ổ cứng gắn ngoài
 - Điện thoại di động



Mã hóa

- Giúp bảo vệ dữ liệu của bạn
- Cũng giúp hacker, VD: Ransomware
- Bảo vệ dữ liệu khi gửi-nhận
 - HTTP ❌ vs. HTTPS ✓
 - Wireless -> WPA2 (AES)
- Bảo vệ thiết bị
 - Nếu không may bị mất/đánh cắp
 - Thường kết hợp với mã PIN/Password
 - Microsoft Windows - BitLocker
 - Apple MacOS - FileVault



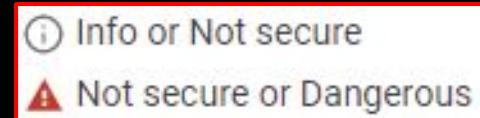
Sử dụng internet an toàn

- Không bao giờ nhấn hoặc cài đặt bất cứ gì từ pop-up bật lên của một trang web
- Các trang web “tin cậy” cũng có thể chứa mã độc
- Cảnh giác: WiFi công cộng, Computers (khách sạn, thư viện...)

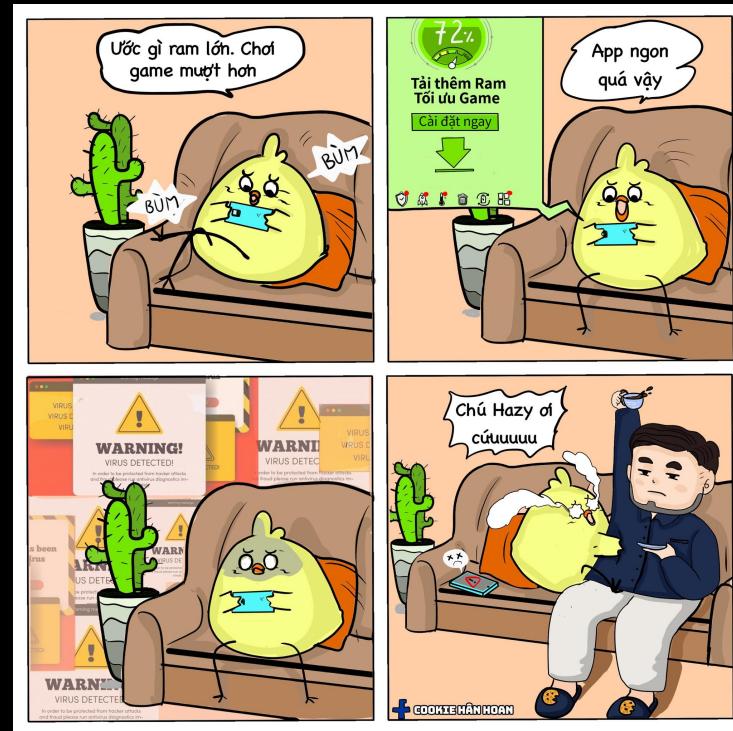
Biểu tượng ổ khóa xanh không có nghĩa là an toàn 100%



Không có ổ khóa



Sử dụng internet an toàn

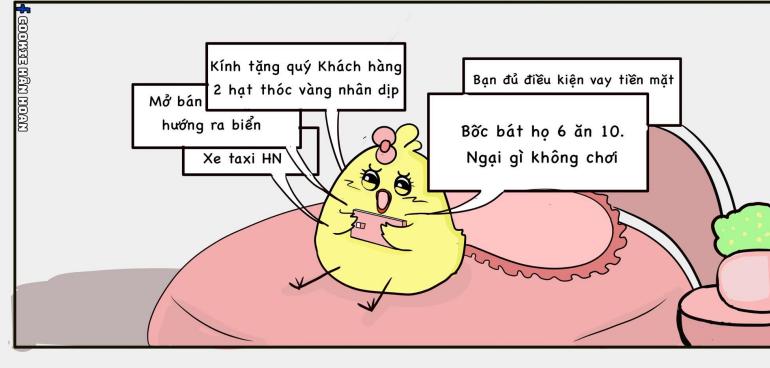


Sử dụng internet an toàn



Sử dụng internet an toàn

Livestream



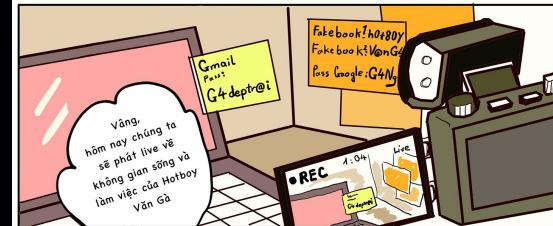
Quyền riêng tư

- Ngày nay dữ liệu về người dùng được coi như “vàng”
- Bạn có đang chia sẻ quá mức không?
 - Các bài khảo sát
 - Chia sẻ thông tin về địa chỉ, vị trí,..
 - Cài đặt quyền riêng tư trên mạng xã hội

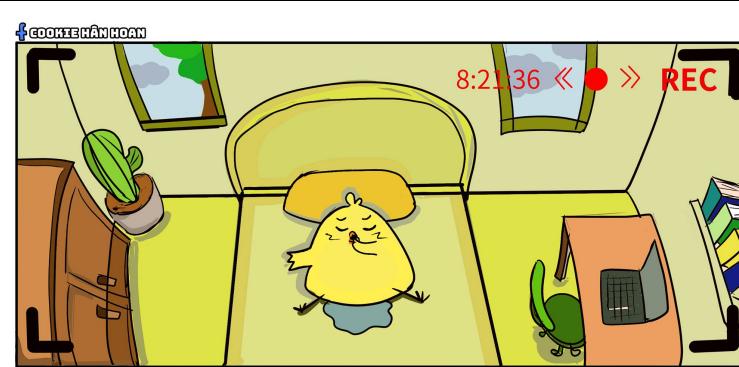
Tôi vừa có ý định mua một cái gì đó ...



Quyền riêng tư



Quyền riêng tư





PHẢI LÀM GÌ KHI GẶP SỰ CỐ ATTT

Làm gì khi gặp sự cố ATTT

- Bình tĩnh, không hoảng sợ
 - Liên hệ ngay với bộ phận hỗ trợ kỹ thuật
 - Viết ra, mô tả lại quá trình gặp sự cố
- **Ransomware**: khóa máy, mã hóa dữ liệu đòi tiền chuộc
 - **Rút mạng? Rút nguồn điện?**
 - Không trả tiền chuộc

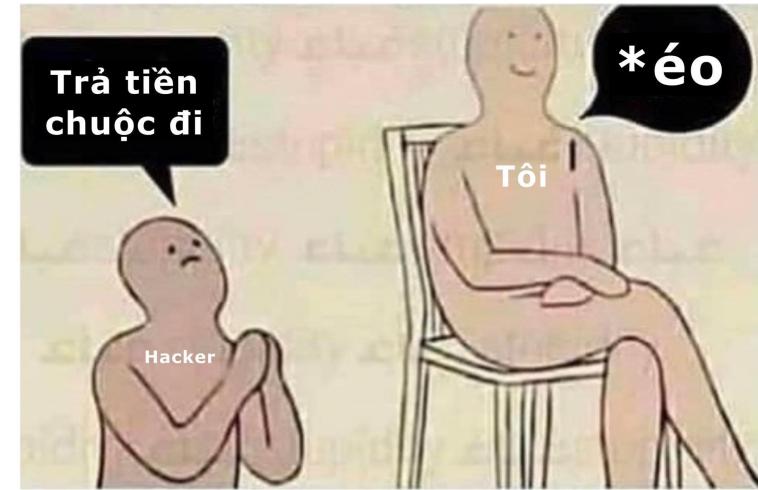


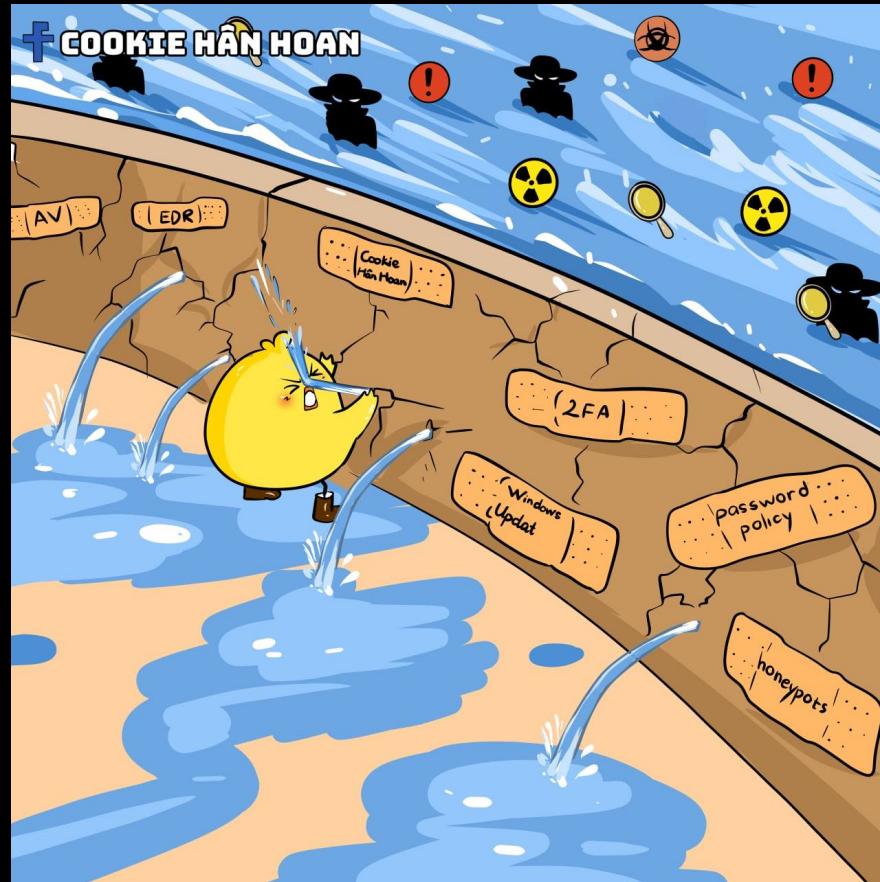
Làm gì khi gặp sự cố ATTT



FACEBOOK HÂN HOAN

**Khi hacker nào đó chiếm đoạt
được dữ liệu của tôi**





Tài liệu tham khảo



- **Báo cáo điều tra vi phạm dữ liệu của Verizon (2021)**
<https://www.verizon.com/business/resources/reports/dbir/>
- **Báo cáo Thị trường An toàn thông tin Việt Nam (2021)**
<http://tailieu.antoanthongtin.gov.vn/Files/files/site-2/files/VCSTT2021.pdf>
- **Báo cáo hoạt động của Ransomware (2021)**
<https://storage.googleapis.com/vtpublic/vt-ransomware-report-2021.pdf>
- Hoạt ảnh:  **Cookie Hân Hoan (@cookie.han.hoan)**

Q&A

