

## CYBERSECURITY & ANTIVIRUS GUIDE / HƯỚNG DẪN BẢO MẬT & DIỆT VIRUS

### ===== MALWARE REMOVAL =====

English:

Steps to remove malware and viruses:

1. Boot into Safe Mode:

- Windows 10/11: Settings > Update & Security > Recovery > Advanced startup > Restart now
- Choose Troubleshoot > Advanced options > Startup Settings > Restart
- Press F4 for Safe Mode or F5 for Safe Mode with Networking

2. Run full antivirus scan:

- Windows Defender: Windows Security > Virus & threat protection > Scan options > Full scan
- Update virus definitions first
- Let scan complete (may take hours)

3. Use additional malware removal tools:

- Malwarebytes: Free scan and removal
- HitmanPro: Secondary opinion scanner
- AdwCleaner: Remove adware and PUPs (Potentially Unwanted Programs)
- RogueKiller: Advanced malware removal

4. Remove suspicious programs:

- Control Panel > Programs and Features
- Sort by installation date
- Uninstall unfamiliar or suspicious programs

5. Reset browser settings:

- Remove suspicious extensions
- Clear cache and cookies
- Reset homepage and search engine
- Chrome: Settings > Reset settings > Restore settings to defaults

6. Check startup programs:

- Task Manager > Startup tab
- Disable suspicious entries
- msconfig > Startup tab (older Windows)

7. Delete temporary files:

- Run Disk Cleanup
- Delete contents of %TEMP% folder
- Use CCleaner for thorough cleanup

Vietnamese:

Các bước loại bỏ malware và virus:

1. Khởi động vào Safe Mode:

- Windows 10/11: Settings > Update & Security > Recovery > Advanced startup > Restart now
- Chọn Troubleshoot > Advanced options > Startup Settings > Restart
- Nhấn F4 cho Safe Mode hoặc F5 cho Safe Mode with Networking

2. Chạy quét toàn bộ antivirus:

- Windows Defender: Windows Security > Virus & threat protection > Scan options > Full scan
- Cập nhật định nghĩa virus trước
- Để quét hoàn thành (có thể mất vài giờ)

3. Dùng công cụ diệt malware bổ sung:

- Malwarebytes: Quét và loại bỏ miễn phí
- HitmanPro: Scanner thứ hai
- AdwCleaner: Loại bỏ adware và PUPs
- RogueKiller: Loại bỏ malware nâng cao

4. Gỡ chương trình đáng ngờ:

- Control Panel > Programs and Features
- Sắp xếp theo ngày cài đặt
- Gỡ các chương trình không quen hoặc đáng ngờ

5. Reset cài đặt trình duyệt:

- Gỡ extensions đáng ngờ
- Xóa cache và cookies
- Reset homepage và search engine
- Chrome: Settings > Reset settings > Restore settings to defaults

6. Kiểm tra chương trình khởi động:

- Task Manager > tab Startup
- Tắt các mục đáng ngờ
- msconfig > tab Startup (Windows cũ)

7. Xóa file tạm:

- Chạy Disk Cleanup
- Xóa nội dung thư mục %TEMP%
- Dùng CCleaner để dọn dẹp kỹ

===== RANSOMWARE PREVENTION & RECOVERY =====

English:

Protecting against and recovering from ransomware:

**Prevention:**

**1. Regular backups:**

- Use 3-2-1 backup rule: 3 copies, 2 different media, 1 offsite
- Enable Windows File History
- Use cloud backup services (OneDrive, Google Drive, Backblaze)
- Keep backup drives disconnected when not in use

**2. Security measures:**

- Keep Windows and all software updated
- Use strong antivirus with ransomware protection
- Enable Windows Defender Ransomware Protection (Controlled Folder Access)
- Don't open suspicious email attachments
- Don't click unknown links

**3. Email security:**

- Be cautious of phishing emails
- Verify sender before opening attachments
- Hover over links to see actual URL
- Look for grammar mistakes and urgency tactics

**If infected:**

1. Disconnect from network immediately
2. Don't pay ransom (no guarantee of file recovery)
3. Identify ransomware variant using ID Ransomware
4. Check for decryption tools: No More Ransom Project
5. Restore from backup if available
6. Report to authorities (FBI IC3, local police)

**Vietnamese:**

Phòng ngừa và khôi phục từ ransomware:

Phòng ngừa:

**1. Sao lưu định kỳ:**

- Dùng quy tắc 3-2-1: 3 bản copy, 2 loại phương tiện khác nhau, 1 ở ngoài
- Bật Windows File History
- Dùng dịch vụ backup cloud
- Giữ ổ backup ngắt kết nối khi không dùng

**2. Biện pháp bảo mật:**

- Cập nhật Windows và phần mềm
- Dùng antivirus mạnh có bảo vệ ransomware
- Bật Windows Defender Ransomware Protection
- Không mở file đính kèm đáng ngờ
- Không click link không rõ nguồn gốc

### 3. Bảo mật email:

- Cẩn thận với email lừa đảo
- Xác minh người gửi trước khi mở file đính kèm
- Di chuột qua link để xem URL thực
- Chú ý lỗi ngữ pháp và chiến thuật gây gẩn rứt

Nếu bị nhiễm:

1. Ngắt kết nối mạng ngay lập tức
2. Không trả tiền chuộc
3. Xác định biến thể ransomware qua ID Ransomware
4. Tìm công cụ giải mã: No More Ransom Project
5. Khôi phục từ backup nếu có
6. Báo cáo với cơ quan chức năng

===== PHISHING AWARENESS =====

English:

Identifying and avoiding phishing attacks:

Common phishing indicators:

#### 1. Suspicious sender email address

- Look for misspellings (paypa1.com instead of paypal.com)
- Generic email addresses (@gmail.com for banks)
- Slightly altered domain names

#### 2. Urgent or threatening language

- "Your account will be closed"
- "Immediate action required"
- "Suspicious activity detected"

#### 3. Generic greetings

- "Dear Customer" instead of your name
- "Dear Sir/Madam"

#### 4. Poor grammar and spelling errors

#### 5. Suspicious links

- Hover to see actual URL
- Shortened URLs (bit.ly) hiding real destination
- URLs with misspellings

#### 6. Unexpected attachments

- Especially .exe, .zip, .scr files
- Invoices you didn't request
- Documents requiring macros

**Protection measures:**

- Never click links in suspicious emails
- Go directly to website by typing URL
- Enable 2-factor authentication
- Verify requests by calling official number
- Report phishing emails
- Use email filtering and anti-phishing tools

**Vietnamese:**

Nhận biết và tránh tấn công phishing:

**Dấu hiệu phishing phổ biến:**

**1. Địa chỉ email người gửi đáng ngờ**

- Tìm lỗi chính tả (paypa1.com thay vì paypal.com)
- Email chung chung (@gmail.com cho ngân hàng)
- Tên miền thay đổi nhẹ

**2. Ngôn ngữ khẩn cấp hoặc đe dọa**

- "Tài khoản sẽ bị đóng"
- "Yêu cầu hành động ngay lập tức"
- "Phát hiện hoạt động đáng ngờ"

**3. Lời chào chung chung**

- "Kính gửi Quý khách" thay vì tên bạn

**4. Ngữ pháp kém và lỗi chính tả**

**5. Link đáng ngờ**

- Di chuột để xem URL thực
- URL rút gọn (bit.ly) che giấu đích đến
- URL có lỗi chính tả

**6. File đính kèm bất ngờ**

- Đặc biệt file .exe, .zip, .scr
- Hóa đơn bạn không yêu cầu
- Tài liệu yêu cầu macros

**Biện pháp bảo vệ:**

- Không bao giờ click link trong email đáng ngờ
- Vào website trực tiếp bằng cách gõ URL
- Bật xác thực 2 yếu tố
- Xác minh yêu cầu bằng cách gọi số chính thức
- Báo cáo email phishing
- Dùng công cụ lọc email và chống phishing

## ===== PASSWORD SECURITY =====

English:

Best practices for password security:

Creating strong passwords:

1. Length: At least 12-16 characters
2. Complexity: Mix of uppercase, lowercase, numbers, symbols
3. Avoid: Dictionary words, personal info, common patterns
4. Use passphrases: "Coffee!Morning@2024\$Fresh"

Password management:

1. Use unique password for each account
2. Never reuse passwords
3. Use password manager (Bitwarden, LastPass, 1Password)
4. Enable 2-factor authentication (2FA)
5. Use authenticator apps instead of SMS when possible

What to do if password is compromised:

1. Change password immediately
2. Enable 2FA if not already active
3. Check for unauthorized access/changes
4. Review connected apps and devices
5. Monitor account for suspicious activity
6. Change passwords on accounts using same password

Password recovery tips:

1. Set up recovery email and phone
2. Save backup codes in secure location
3. Don't share recovery information
4. Keep recovery information updated

Vietnamese:

Thực hành tốt nhất về bảo mật mật khẩu:

Tạo mật khẩu mạnh:

1. Độ dài: Ít nhất 12-16 ký tự
2. Phức tạp: Kết hợp chữ hoa, chữ thường, số, ký tự đặc biệt
3. Tránh: Từ điển, thông tin cá nhân, mẫu phổ biến
4. Dùng cụm từ: "CaPhe!Sang@2024\$TuoiMoi"

Quản lý mật khẩu:

1. Dùng mật khẩu riêng cho mỗi tài khoản
2. Không bao giờ dùng lại mật khẩu

3. Dùng trình quản lý mật khẩu
4. Bật xác thực 2 yếu tố (2FA)
5. Dùng ứng dụng authenticator thay vì SMS khi có thể

Làm gì khi mật khẩu bị lộ:

1. Đổi mật khẩu ngay lập tức
2. Bật 2FA nếu chưa có
3. Kiểm tra truy cập/thay đổi trái phép
4. Xem lại ứng dụng và thiết bị kết nối
5. Theo dõi hoạt động đáng ngờ
6. Đổi mật khẩu các tài khoản dùng cùng mật khẩu

Mẹo khôi phục mật khẩu:

1. Thiết lập email và số điện thoại khôi phục
2. Lưu mã backup ở nơi an toàn
3. Không chia sẻ thông tin khôi phục
4. Giữ thông tin khôi phục được cập nhật

## ===== FIREWALL & SECURITY SETTINGS =====

English:

Configuring Windows Firewall and security settings:

Windows Firewall:

1. Enable Windows Firewall:
  - Settings > Update & Security > Windows Security > Firewall & network protection
  - Ensure all networks (Domain, Private, Public) have firewall ON
2. Allow app through firewall:
  - Click "Allow an app through firewall"
  - Find your application
  - Check appropriate network types
3. Create firewall rules:
  - Windows Defender Firewall > Advanced settings
  - Inbound/Outbound Rules > New Rule
  - Specify port, program, or service

Windows Security settings:

1. Virus & threat protection:
  - Enable real-time protection
  - Enable cloud-delivered protection
  - Enable automatic sample submission
2. Ransomware protection:

- Turn on Controlled folder access
- Add protected folders
- Allow apps through controlled folder access

### 3. Account protection:

- Set up Windows Hello (PIN, fingerprint, face recognition)
- Enable Dynamic lock

### 4. App & browser control:

- Enable SmartScreen for apps and files
- Enable SmartScreen for Microsoft Edge

Vietnamese:

Cấu hình Windows Firewall và cài đặt bảo mật:

Windows Firewall:

#### 1. Bật Windows Firewall:

- Settings > Update & Security > Windows Security > Firewall & network protection
- Đảm bảo tất cả mạng có firewall BẬT

#### 2. Cho phép ứng dụng qua firewall:

- Click "Allow an app through firewall"
- Tìm ứng dụng của bạn
- Tích các loại mạng phù hợp

#### 3. Tạo quy tắc firewall:

- Windows Defender Firewall > Advanced settings
- Inbound/Outbound Rules > New Rule
- Chỉ định cổng, chương trình hoặc dịch vụ

Cài đặt Windows Security:

#### 1. Bảo vệ virus & mối đe dọa:

- Bật real-time protection
- Bật cloud-delivered protection
- Bật automatic sample submission

#### 2. Bảo vệ ransomware:

- Bật Controlled folder access
- Thêm thư mục được bảo vệ
- Cho phép ứng dụng qua controlled folder access

#### 3. Bảo vệ tài khoản:

- Thiết lập Windows Hello
- Bật Dynamic lock

4. Kiểm soát ứng dụng & trình duyệt:

- Bật SmartScreen cho apps và files
- Bật SmartScreen cho Microsoft Edge