

**SỞ THÔNG TIN VÀ TRUYỀN THÔNG LONG AN
HỘI TIN HỌC**

CHỦ ĐỀ

BẢO VỆ KHỎI NGUY CƠ MÃ ĐỘC

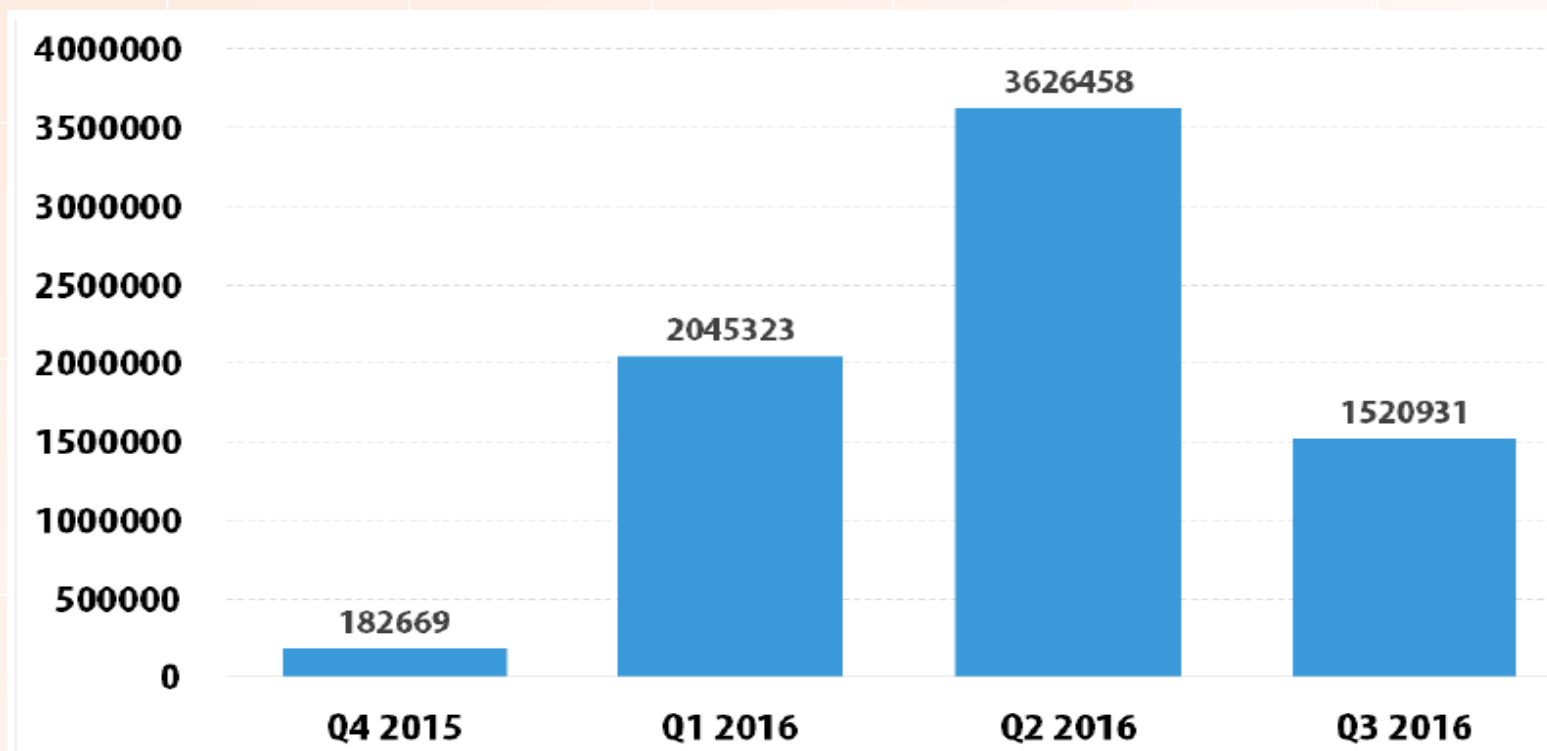
**Trình bày: Th.s Nguyễn Mai Tuấn Khoa
Trung tâm Công nghệ thông tin và Truyền thông**

NỘI DUNG

- 1. Mã độc và những con số**
- 2. Mã độc, công cụ của tội phạm mạng**
- 3. Nguyên nhân lây nhiễm mã độc**
- 4. Những biện pháp phòng ngừa**

MÃ ĐỘC VÀ NHỮNG CON SỐ

Số lượng các gói cài đặt có kèm mã độc trên điện thoại di động



(Nguồn IT Threat Evolution In Q3 2016 – Kaspersky)

MÃ ĐỘC VÀ NHỮNG CON SỐ

Việt Nam là quốc gia có nguy cơ cao nhất lây nhiễm mã độc trong mạng nội bộ

	Country*	% of users attacked**
1	Vietnam	52.07
2	Afghanistan	52.00
3	Yemen	51.32
4	Somalia	50.78
5	Ethiopia	50.50
6	Uzbekistan	50.15
7	Rwanda	50,14
8	Laos	49.27
9	Venezuela	49.27
10	Philippines	47.69

(Nguồn IT Threat Evolution In Q3 2016 – Kaspersky)

MÃ ĐỘC, CÔNG CỤ CỦA TỘI PHẠM

Những biến thể của mã độc



MÃ ĐỘC, CÔNG CỤ CỦA TỘI PHẠM

Mục tiêu của mã độc



MÃ ĐỘC, CÔNG CỤ CỦA TỘI PHẠM

Đối tượng lây nhiễm



MÃ ĐỘC, CÔNG CỤ CỦA TỘI PHẠM

Phương thức lây nhiễm



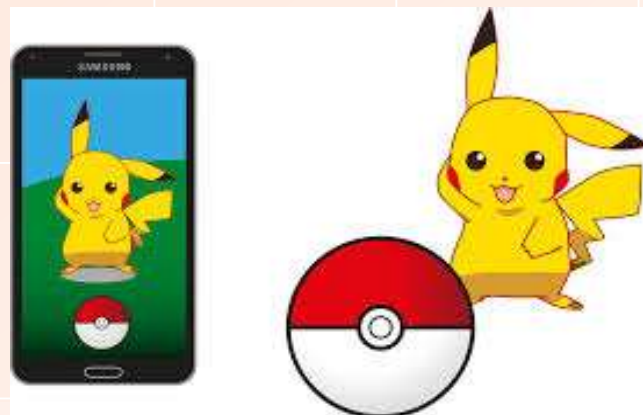
MÃ ĐỘC, CÔNG CỤ CỦA TỘI PHẠM

Phương thức lây nhiễm



MÃ ĐỘC, CÔNG CỤ CỦA TỘI PHẠM

Phương thức lây nhiễm



NGUYÊN NHÂN LÂY NHIỄM MÃ ĐỘC

Khách quan

Windows Update

 **Some updates were not installed**

Failed: 3 updates
[Review important updates](#)
[Review optional updates](#) Try again

3 important updates selected

Error(s) found:

Code 80070003: Windows Update ran into a problem. [Get help with this error](#)
Code 8004200D: Windows Update ran into a problem. [Get help with this error](#)

Most recent check for updates: 7/12/2013 at 9:16 PM
Updates were installed: Today at 10:00 PM (Failed).
You receive updates: For Windows and other products from Microsoft Update.

 **"Adobe Flash Player" is out-of-date**

The version of this plug-in on your computer does not include the latest security updates and is blocked. To continue using "Adobe Flash Player", download an update from Adobe.

[Download Flash...](#) OK

Your computer is out of date.



We detected that your computer is out of date. We suggest you to update by installing [office](#) [tools](#). They will improve your productivity and make your computer up to date. You can check policy and privacy of all of [tools](#). Only some of them compatible between each other and current installed applications in

OK

 Microsoft

We detected your browser is NOT up-to-date.

Old and outdated browser versions have security issues and don't follow the new web development standards. Update your browser enforcing the international movement to eliminate the obsolete browser versions.

Update browser

These buttons link to the official browser webpages. You can choose platform and language there.

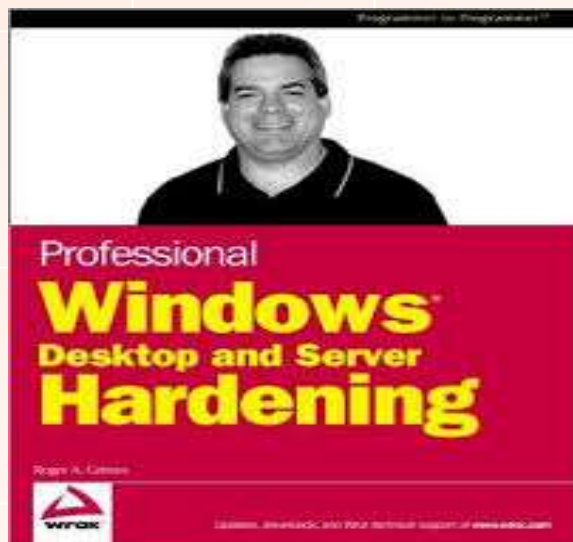
 **Google Chrome**
For PC, Mac + Linux
[Download free](#) 

 **Internet Explorer**
For PC, Mac + Linux
[Download free](#) 

 **Firefox**
For PC, Mac + Linux
[Download free](#) 

NGUYÊN NHÂN LÂY NHIỄM MÃ ĐỘC

Khách quan



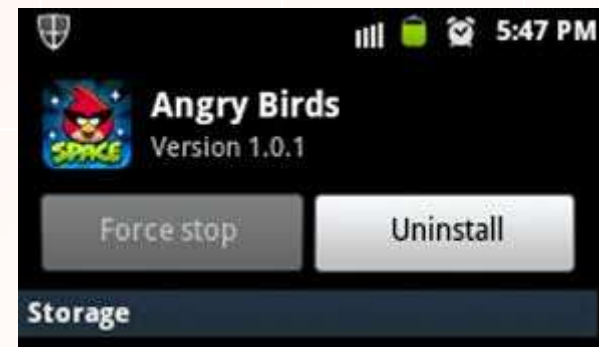
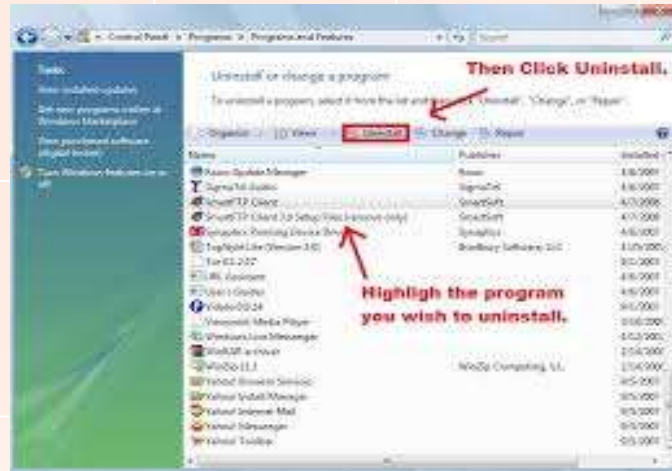
NGUYÊN NHÂN LÂY NHIỄM MÃ ĐỘC

Chủ quan



NHỮNG BIỆN PHÁP PHÒNG NGỪA

Xóa những ứng dụng không cần thiết



NHỮNG BIỆN PHÁP PHÒNG NGỪA

Sử dụng phần mềm diệt virus



ANTIVIRUS



FIREWALL



NHỮNG BIỆN PHÁP PHÒNG NGỪA

Luôn cập nhật bản vá phần mềm, hệ điều hành


- ✓ Định kỳ cập nhật bản vá lỗi phần mềm, hệ điều hành, chương trình diệt virus,...
- ✓ Nhận biết những khác thường trong quá trình sử dụng: máy khởi động chậm, hệ thống hoạt động không ổn định,...



NHỮNG BIỆN PHÁP PHÒNG NGỪA

An toàn khi giao dịch trực tuyến

- ✓ Kiểm tra chữ “s” trên địa chỉ website, hạn chế đánh cắp thông tin
- ✓ Kết nối an toàn,...
- ✓ Xác thực mạnh,...

 ỦY BAN NHÂN DÂN TỈNH LONG AN... (VN) | <https://mail.longan.gov.vn/c>



NHỮNG BIỆN PHÁP PHÒNG NGỪA

Sử dụng mật khẩu mạnh

- ✓ Thay đổi định kỳ
- ✓ Xác thực mạnh: OTP, sinh trắc học
- ✓ Tự xác lập quy luật dễ nhớ ($a \leftrightarrow @$; $S \leftrightarrow \$$; $o \leftrightarrow 0, \dots$)
- ✓ Mật khẩu dạng câu (HtATTHThtL0ng@n25/11/2016 - Hội thảo ATTT Hội Tin học tỉnh Long An 25/11/2016)
- ✓ Sử dụng ít nhất 8 ký tự bao gồm ký tự hoa, thường, ký tự số, ký tự đặc biệt,...

NHỮNG BIỆN PHÁP PHÒNG NGỪA

Hạn chế đăng nhập khi sử dụng wifi công cộng



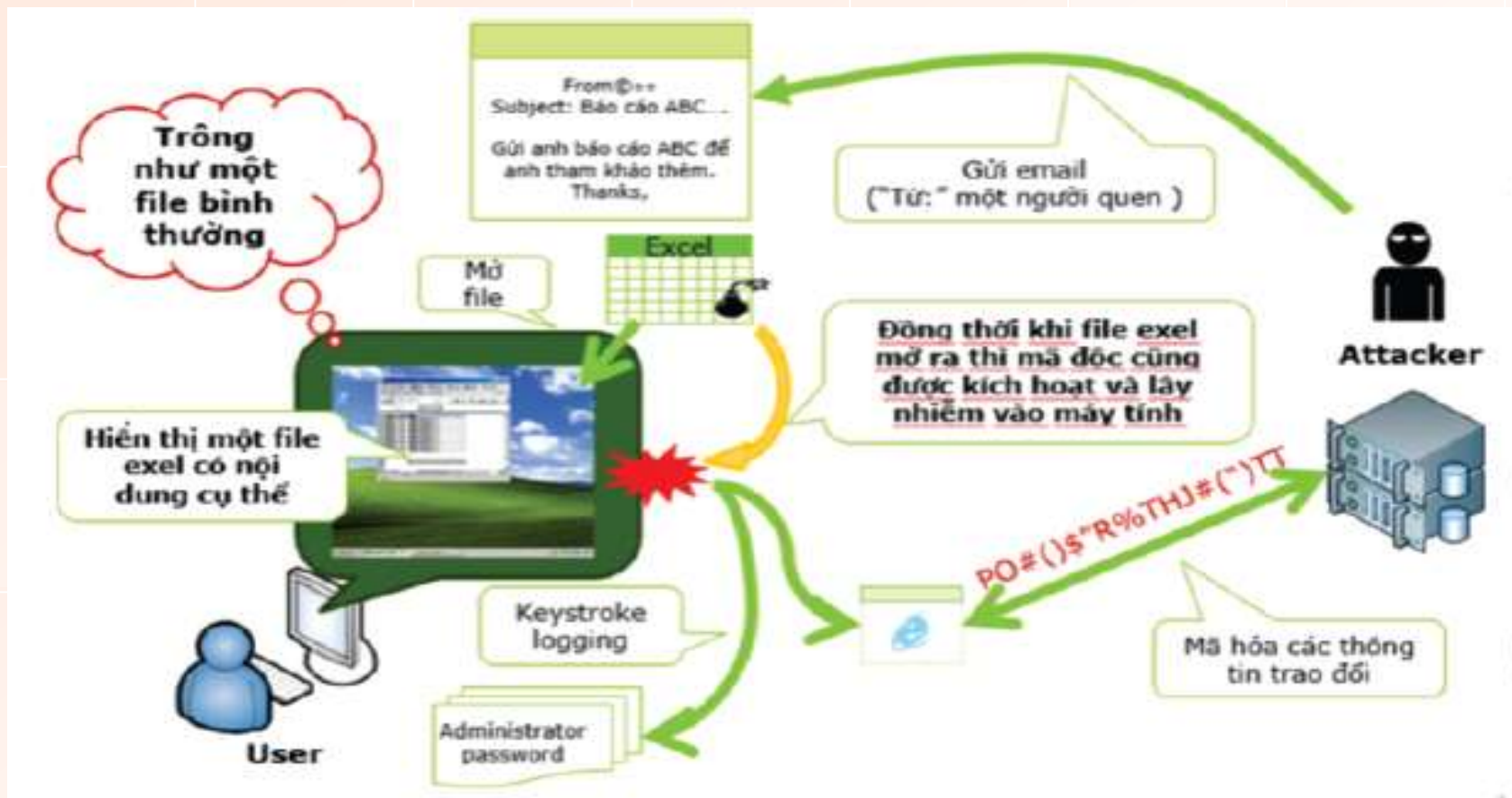
NHỮNG BIỆN PHÁP PHÒNG NGỪA

Không nên tin tưởng tên hiển thị trên email



NHỮNG BIỆN PHÁP PHÒNG NGỪA

Cần nhắc khi tải file trên email



NHỮNG BIỆN PHÁP PHÒNG NGỪA

Cẩn trọng khi truy cập các trang web lạ



NHỮNG BIỆN PHÁP PHÒNG NGỪA

Không sử dụng phần mềm bẻ khóa



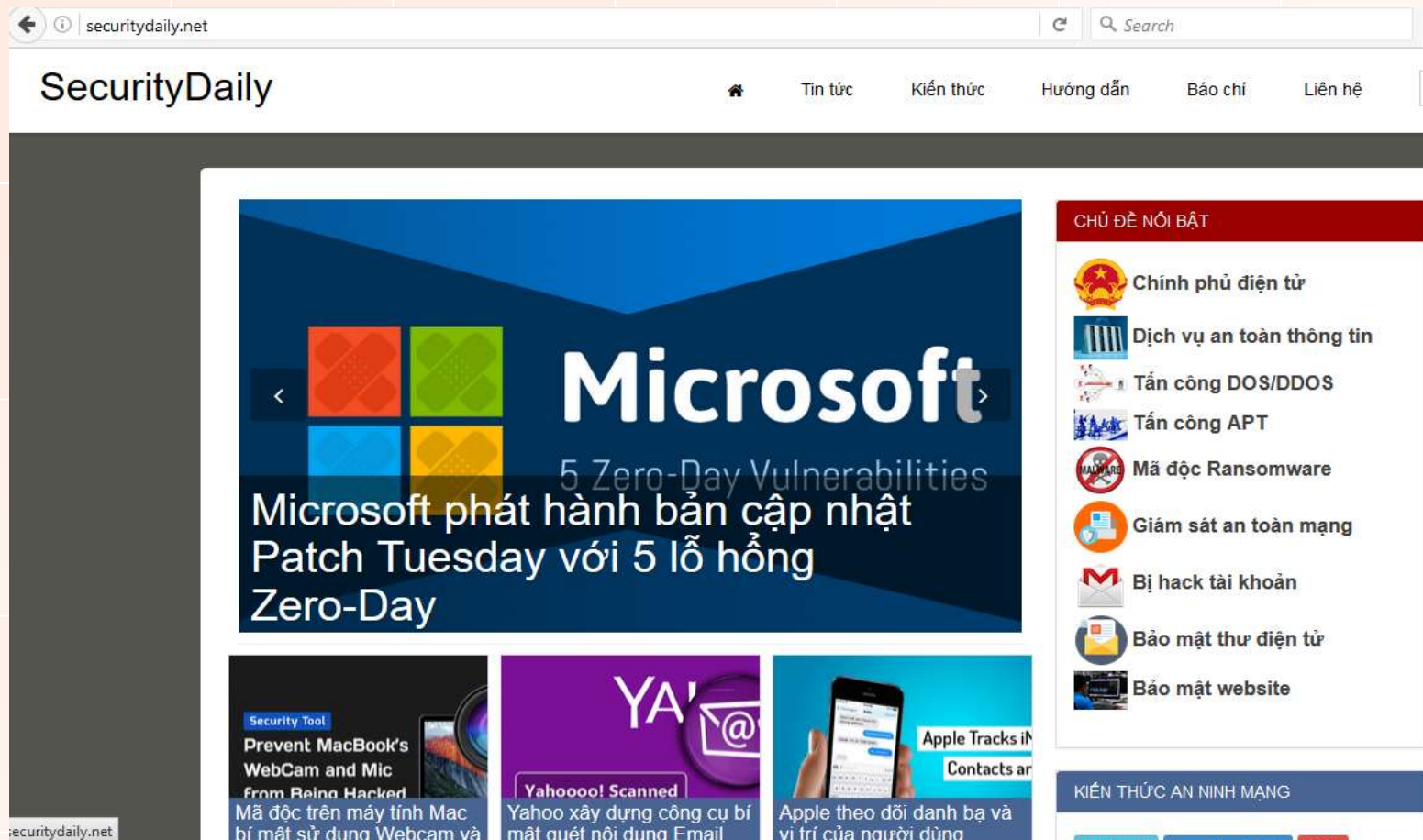
NHỮNG BIỆN PHÁP PHÒNG NGỪA

Tuân thủ các quy định về ATTT

- ✓ Tuân thủ các quy định về vận hành hệ thống, kiểm tra thư điện tử, quét virus, cập nhật chương trình, hệ điều hành, triển khai hệ thống mạng không dây,...
- ✓ Việc cài đặt các ứng dụng, sửa chữa máy tính phải tuân theo quy định của đơn vị,...
- ✓ Nâng cao nhận thức về an toàn thông tin, nhận dạng các phương pháp tấn công để có biện pháp bảo vệ thích hợp
- ✓ Thường xuyên cập nhật các kiến thức về an toàn thông tin qua sách báo, mạng internet, báo cáo chuyên đề ATTT

NHỮNG BIỆN PHÁP PHÒNG NGỪA

Cập nhật kiến thức



The screenshot shows the SecurityDaily website interface. The main content area features a large article titled "Microsoft phát hành bản cập nhật Patch Tuesday với 5 lỗ hổng Zero-Day" (Microsoft releases Patch Tuesday update with 5 Zero-Day vulnerabilities). The article includes a Microsoft logo and the text "5 Zero-Day Vulnerabilities".

The sidebar on the right, titled "CHỦ ĐỀ NỔI BẬT" (Trending Topics), lists several security-related items:

- Chính phủ điện tử (E-Government)
- Dịch vụ an toàn thông tin (Information Security Service)
- Tấn công DOS/DDOS (DOS/DDOS Attack)
- Tấn công APT (APT Attack)
- Mã độc Ransomware (Ransomware)
- Giám sát an toàn mạng (Network Security Monitoring)
- Bị hack tài khoản (Account Hacked)
- Bảo mật thư điện tử (Email Security)
- Bảo mật website (Website Security)

Below the main article, there are three smaller featured articles:

- Security Tool**: Prevent MacBook's WebCam and Mic From Being Hacked. Mã độc trên máy tính Mac bí mật sử dụng Webcam và...
- YAHOO!**: Yahoooooo! Scanned. Yahoo xây dựng công cụ bí mật quét nội dung Email
- Apple Tracks i**: Apple theo dõi danh bạ và vị trí của người dùng

NHỮNG BIỆN PHÁP PHÒNG NGỪA

Cập nhật kiến thức



The screenshot shows a web browser window with the URL ictnews.vn. The page features a navigation bar with icons for various mobile devices: a laptop, a smartphone, a tablet, an iPhone, several other smartphones, and a feature phone. Below the navigation bar, there are two main news items:


- Mới nhất:** chương trình “Sự phụ - Đệ tử” tại FSB
- FPT Shop bất ngờ cho khách đổi điện thoại Samsung cũ lấy máy mới

The main content area is divided into three columns, each with an image and a text block:

- Column 1:** Image of a meeting around a long table. Text: **Điện thoại cố định được tạo điều kiện phát triển trước “cơn bão” di động**. Subtext: ICTnews - Trước xu thế liên tục bị suy giảm do nhu cầu sử dụng điện thoại di động của người dân tăng cao, chính sách của Việt Nam luôn tạo điều kiện để điện thoại cố định duy trì
- Column 2:** Image of a man speaking. Text: **Đổi mã vùng điện thoại cố định: Bộ TT&TT, các nhà mạng đã chuẩn bị rất kỹ lưỡng**
- Column 3:** Image of a man at a podium. Text: **“Dừng dự án điện hạt nhân Ninh Thuận không phải vì lý do công nghệ không an toàn”**

NHỮNG BIỆN PHÁP PHÒNG NGỪA

Cập nhật kiến thức



The screenshot shows the website **quantrimang.com** with the following elements:

- Header:** Logo of Quantrimang (Kiến thức - Kinh nghiệm - Hỏi đáp) and a search bar with the text "Google™ Tìm kiếm Tuy Chính".
- Navigation Bar:** Links for Trang chủ, Công nghệ, Khoa học, Điện máy, Cuộc sống, Video, Ứng dụng, and iPhone / iPad.
- Left Sidebar (Công nghệ):**
 - Ứng dụng
 - Hệ thống
 - Game - Trò chơi
 - iPhone / iPad
 - Android
 - Windows Phone
 - Mac OS X
 - Chụp ảnh - Quay p...
 - Phần cứng
 - Thủ thuật SEO
 - Kiến thức cơ bản
- Main Content Area:**
 - Featured Article:** "Cách ngăn chặn hình ảnh .SVG chứa mã độc mới trên Facebook" (How to prevent new .SVG images containing malware on Facebook). The image shows the Facebook logo with cartoonish viruses.
 - Advertisement:** "Internet 12M chỉ 150.000đ" (12M Internet for only 150,000 VND) with details: "K.Mãi Internet Cáp quang siêu tốc 12M chỉ 150K, Miễn phí WIFI 4 port Truy cập vào fibervnn.vn/K_mai_internet".
 - Footer:** "Quảng cáo của Google" and navigation links: "Quản lý", "Mạng", "Máy cơ mạng".

Four realistic water droplets are positioned above the text, appearing to fall or have just landed. The background features a light beige grid pattern on the left and a colorful abstract design on the right with segments in blue, red, yellow, and green.

**CẢM ƠN
ĐÃ CHÚ Ý LẮNG NGHE !!!**