SỞ THÔNG TIN VÀ TRUYỀN THÔNG LONG AN
HỘI TIN HỌC

CHỦ ĐỀ

BẢO VỆ KHỎI NGUY CƠ MÃ ĐỘC

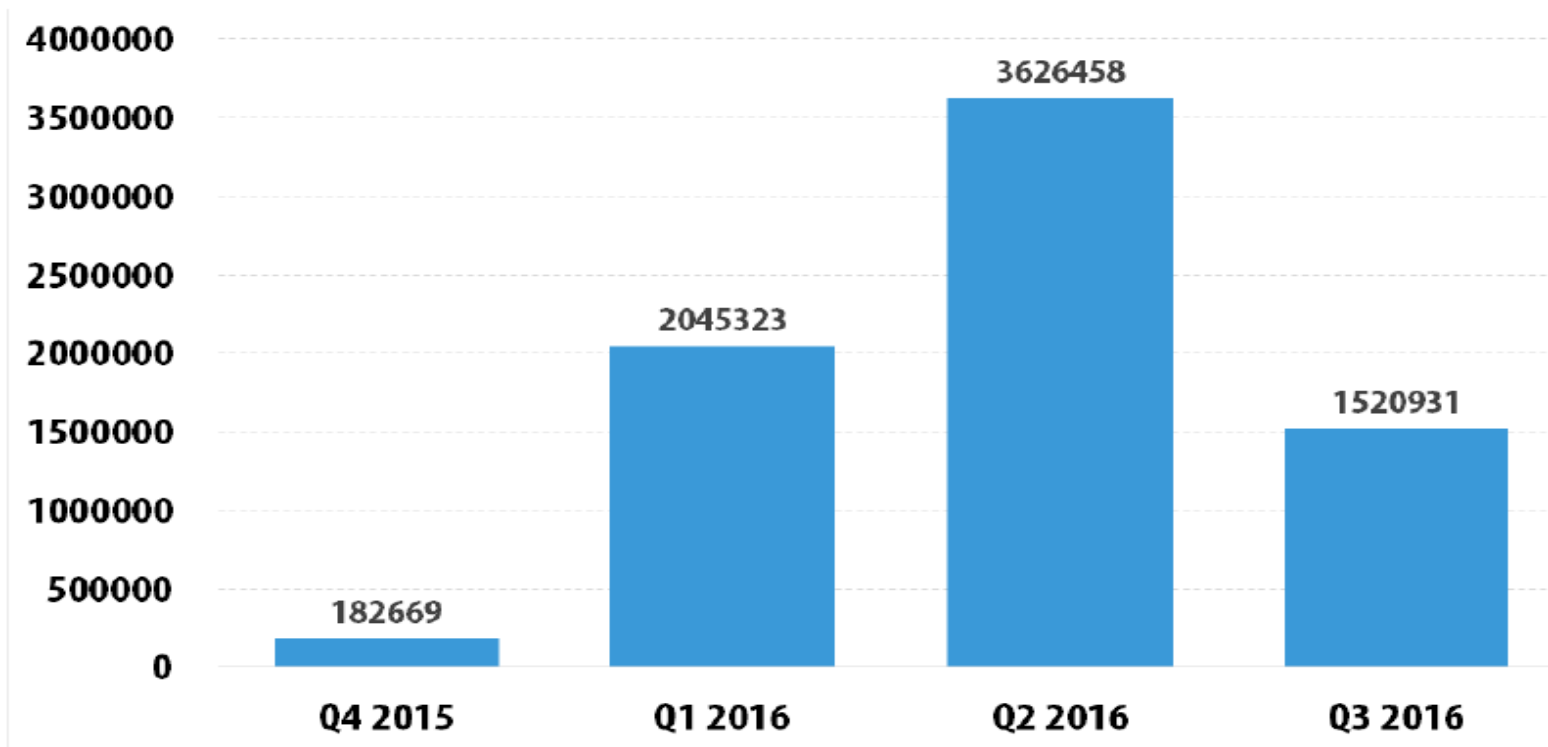
Trình bày: Th.s Nguyễn Mai Tuấn Khoa
Trung tâm Công nghệ thông tin và Truyền thông

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

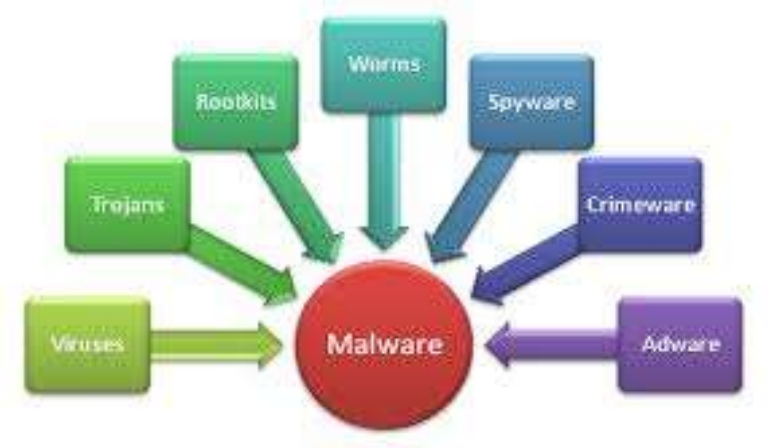
Việt Nam là quốc gia có nguy cơ cao nhất lây nhiễm mã độc trong mạng nội bộ

	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

Mã độc là gì?



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

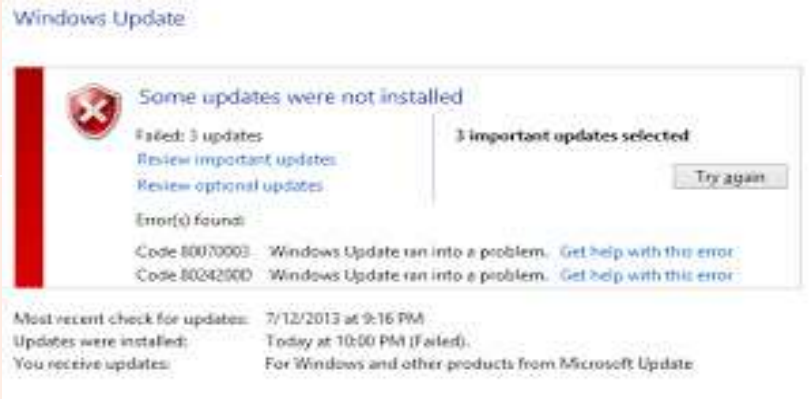
Phương thức lây nhiễm

MÃ ĐỘC, CÔNG CỤ CỦA TỘI PHẠM

Phương thức lây nhiễm

NGUYÊN NHÂN LÂY NHIỄM MÃ ĐỘC

Khách quan



NGUYÊN NHÂN LÂY NHIỄM MÃ ĐỘC

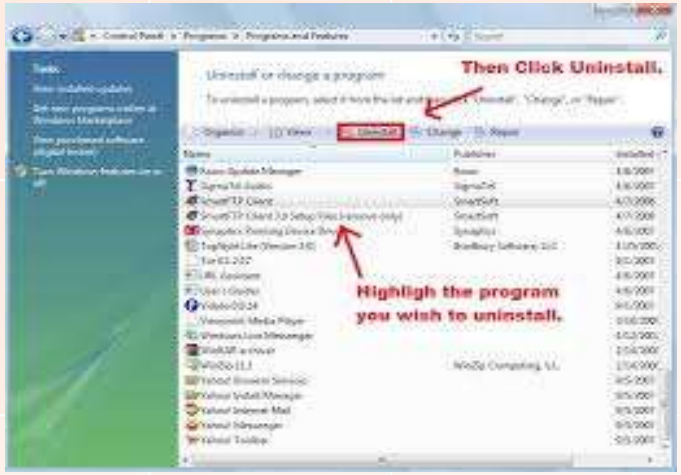
Khách quan

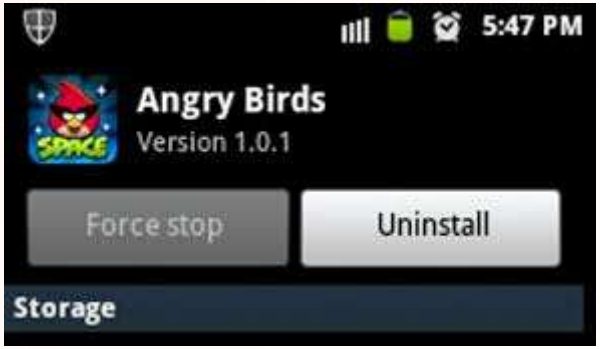
NGUYÊN NHÂN LÂY NHIỄM MÃ ĐỘC

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

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,...

NHỮNG BIỆN PHÁP PHÒNG NGỪA

Sử dụng mật khẩu mạnh

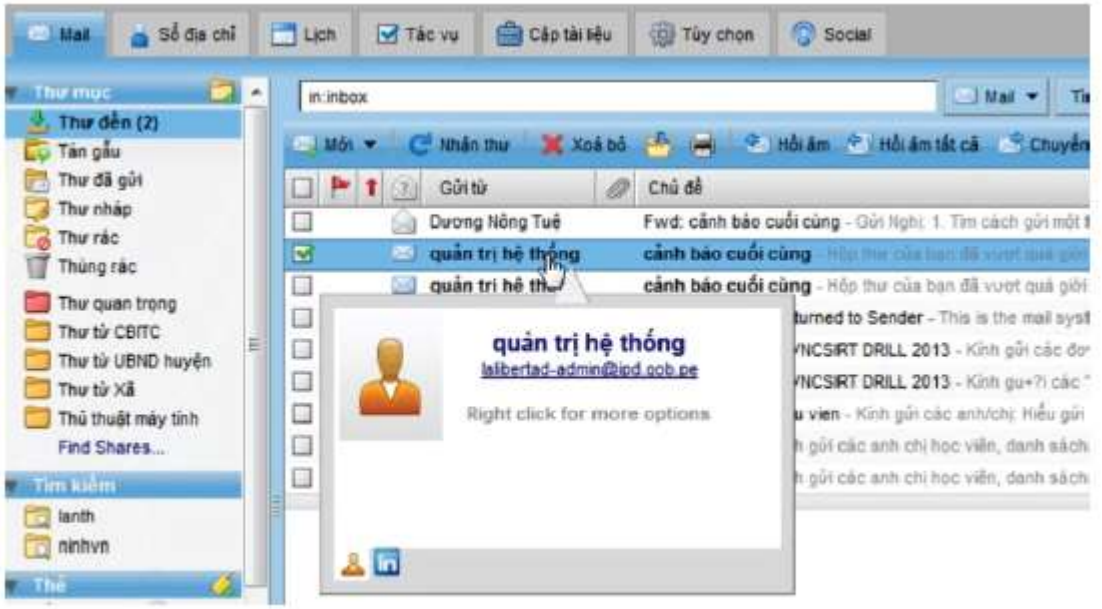
- ✓ Thay đổi định kỳ
- ✓ Xác thực mạnh: OTP, sinh trắc học
- ✓ Tự xác lập quy luật dễ nhớ (a⇔@; S⇔$; o⇔0,…)
- ✓ Mật khẩu dạng câu (HtATTTHThtL0ng@n25/11/2016 - Hội thảo ATTT Hội Tin học tỉnh Long An 25/11/2016)
- ✓ Sử dụng ít nhất 8 ký tự bao gồm ký tự hoa, thường, ký tự số, ký tự đặc biệt,…

NHỮNG BIỆN PHÁP PHÒNG NGỪA

Hạn chế đăng nhập khi sử dụng wifi công cộng

NHỮNG BIỆN PHÁP PHÒNG NGỪA

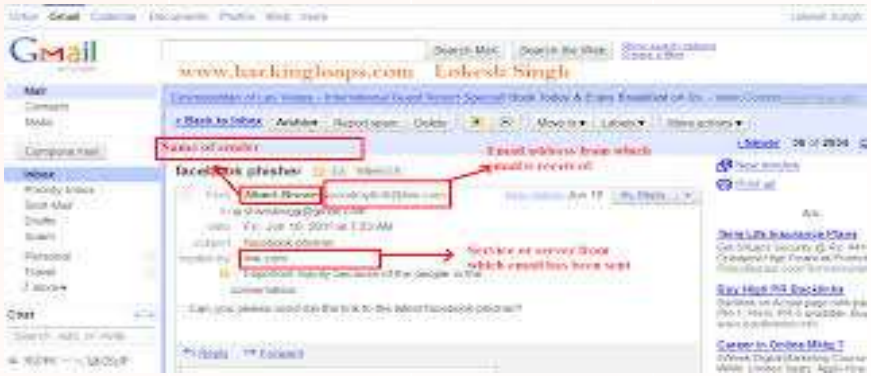
Sử dụng thư điện tử thận trọng



(Ví dụ một thư điện tử giả mạo đính kèm mã độc)

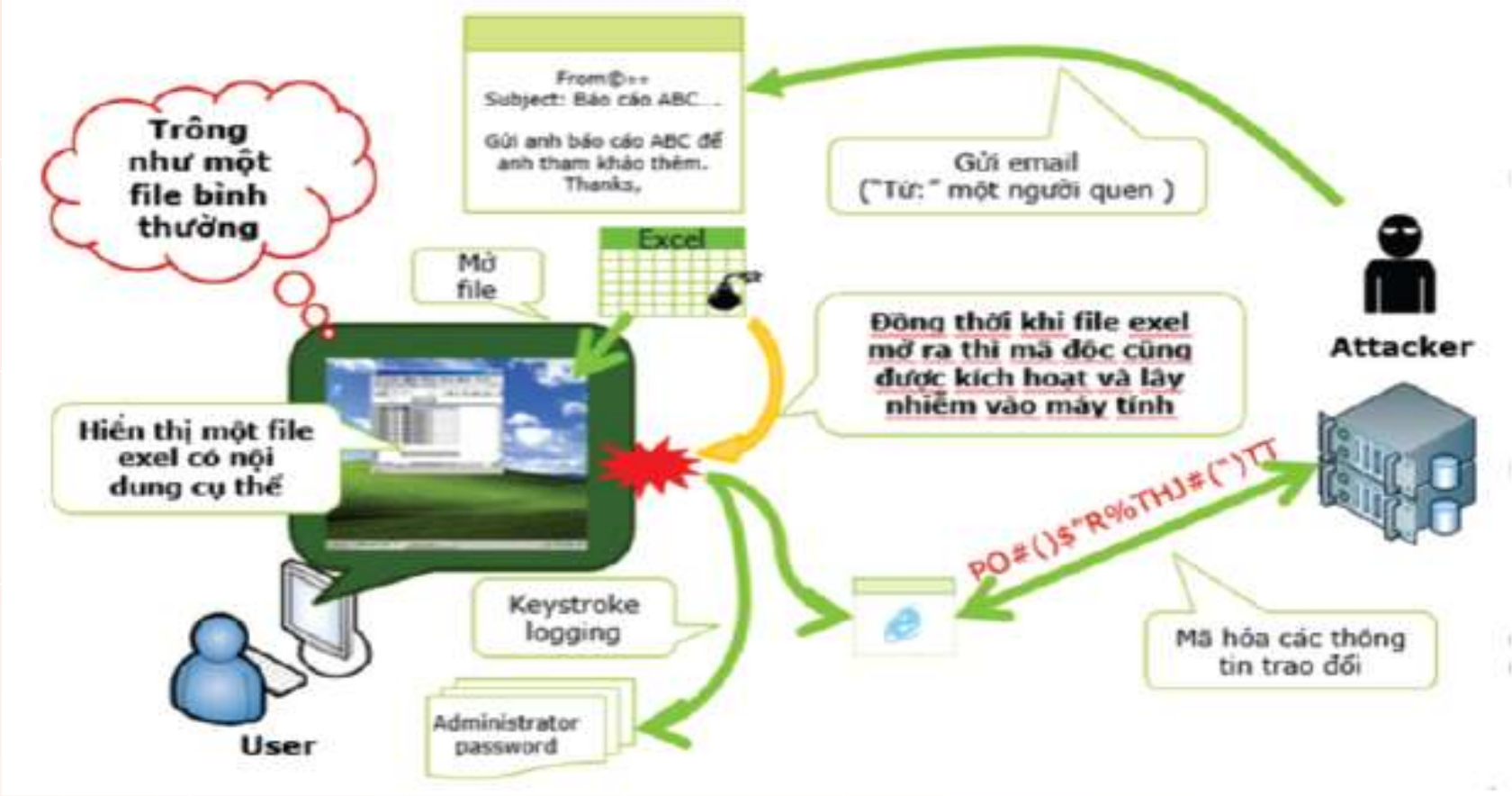
NHỮNG BIỆN PHÁP PHÒNG NGỪA

Không nên tin tưởng tên hiển thị trên email



NHỮNG BIỆN PHÁP PHÒNG NGỪA

Cân 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

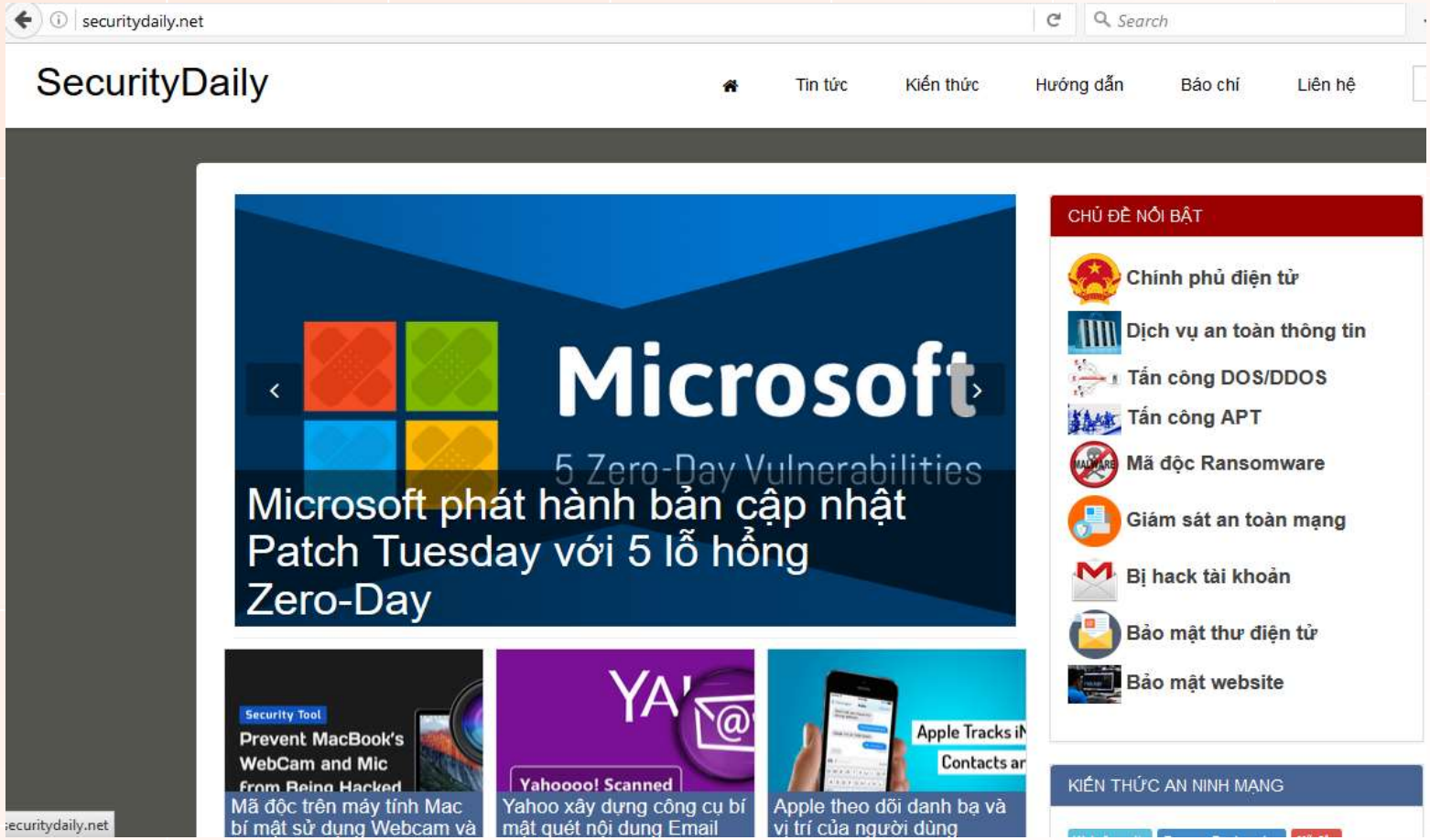
NHỮNG BIỆN PHÁP PHÒNG NGỪA

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

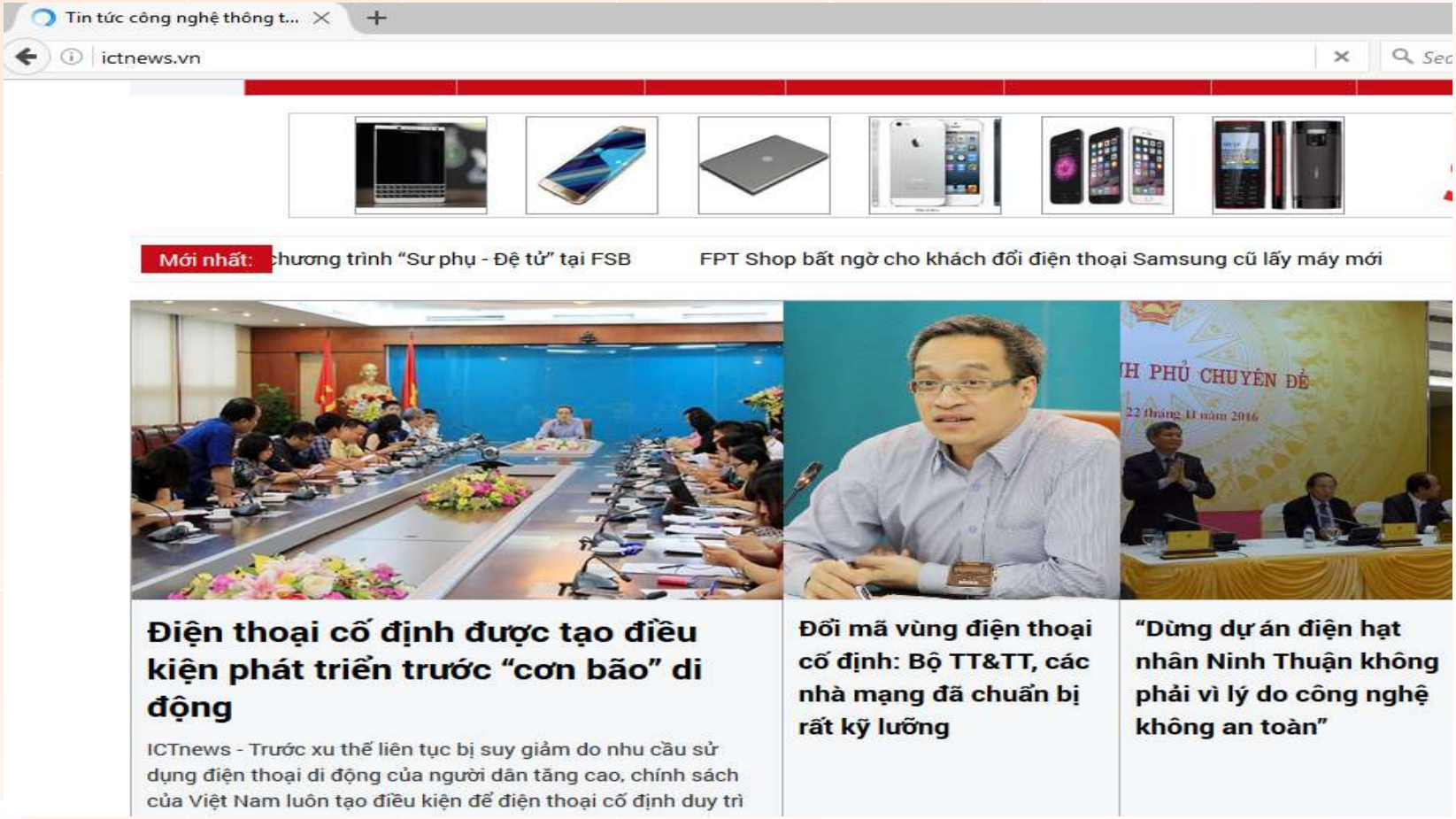
NHỮNG BIỆN PHÁP PHÒNG NGỪA

Cập nhật kiến thức



NHỮNG BIỆN PHÁP PHÒNG NGỪA

Cập nhật kiến thức



NHỮNG BIỆN PHÁP PHÒNG NGỪA

Cập nhật kiến thức

CÁM ƠN
ĐÃ CHÚ Ý LẮNG NGHE !!!