**BẢN TIN NỘI BỘ**

**CẬP NHẬT VỀ AN TOÀN THÔNG TIN VÀ CẢNH BÁO LỖ HỔNG BẢO MẬT**

## 1. Xây dựng thành công Chính phủ điện tử bằng sức mạnh nội tại

Việt Nam đủ khả năng xây dựng Chính phủ điện tử bằng sức mạnh nội tại, dựa trên nguồn lực của nhà nước và tư nhân cùng làm, đó là nhận định của Thủ tướng Nguyễn Xuân Phúc tại Hội nghị Ủy ban Quốc gia về Chính phủ điện tử với Ban chỉ đạo Chính phủ điện tử, chính quyền điện tử bộ, ngành, địa phương diễn ra sáng 12/2.

Tham dự Hội nghị còn có Phó Thủ tướng Chính phủ, Phó Chủ tịch thường trực Ủy ban Quốc gia về Chính phủ điện tử Vũ Đức Đam; Bộ trưởng, Chủ nhiệm Văn phòng Chính phủ Mai Tiến Dũng; Bộ trưởng Bộ Thông tin và Truyền thông Nguyễn Mạnh Hùng; lãnh đạo các bộ, ngành và kết nối trực tuyến đến 63 địa phương.

Đây là Hội nghị trực tuyến lần thứ 3 được tổ chức sau gần 18 tháng thành lập Ủy ban Quốc gia (UBQG) về Chính phủ điện tử (CPĐT) và là Hội nghị toàn quốc đầu tiên sau Tết Canh Tý.

Thủ tướng cho biết, Hội nghị được tổ chức nhằm tổng kết, đánh giá một năm triển khai CPĐT, từ đó lựa chọn kết quả tốt nhất để nhân rộng cách làm và bổ sung, hoàn thiện các giải pháp một cách thực chất. Bên cạnh đó, Hội nghị sẽ thảo luận về các cản trở, khó khăn trong xây dựng CPĐT, nhất là chủ trương các cấp chính quyền hưởng ứng việc đưa toàn dân tham gia xây dựng CPĐT.

CPĐT sẽ tăng cường tính minh bạch và chống tham nhũng, lấy người dân làm trung tâm để không ai bị bỏ lại phía sau. Nhưng nếu người dân không dùng các dịch vụ công thì CPĐT không thành công.

“Chúng ta đưa ra những nhiệm vụ mới, giải pháp mới để năm 2020 thực hiện đạt kết quả tốt, đóng góp vào phát triển kinh tế xã hội của đất nước, vào lộ trình xây dựng CPĐT ở Việt Nam. CPĐT không phải làm một lúc là xong được mà chia làm nhiều giai đoạn, có những giai đoạn quan trọng, trong đó năm 2020 là năm có nhiều thách thức. Chúng ta phải có định hướng như thế nào để triển khai có hiệu quả nhất để tăng năng suất lao động” Thủ tướng nói.

Bên cạnh đó, Thủ tướng nhận định, cả nước đang tích cực triển khai hiệu quả các biện pháp phòng chống dịch bệnh viêm đường hô hấp cấp do chủng virus Corona. Nếu làm tốt CPĐT cũng là một giải pháp ngăn ngừa virus Corona khi hiện nay, nhiều cơ quan, đơn vị, trường học ứng dụng CPĐT trong giao dịch, hạn chế tiếp xúc trực tiếp.

Báo cáo tại Hội nghị, Bộ trưởng Bộ Thông tin và Truyền thông Nguyễn Mạnh Hùng cho biết, năm 2019, công cuộc xây dựng CPĐT có nhiều chuyển biến tích cực. Tỷ lệ dịch vụ công trực tuyến cấp độ 4 tăng gấp đôi. Hệ thống Trục liên thông văn bản quốc gia phục vụ gửi, nhận văn bản điện tử giữa các cơ quan trong hệ thống hành chính Nhà nước; Hệ thống thông tin phục vụ họp và xử lý công việc của Chính phủ; Cổng Dịch vụ công quốc gia đã được khai trương và đi hoạt động đã phát huy hiệu quả bước đầu; công tác bảo đảm an toàn thông tin, an ninh mạng được cải thiện.

Từ thời điểm Thủ tướng Chính phủ nhấn nút khai trương (09/12/2019) đến nay, đã có 47.377 tài khoản đăng ký trên Cổng Dịch vụ công quốc gia; có hơn 13,7 triệu lượt truy cập; hơn 945.000 hồ sơ đồng bộ trạng thái. Đến thời điểm này, đã có 9/22 Bộ, cơ quan và 63/63 tỉnh, thành phố kết nối, tích hợp với Cổng Dịch vụ công quốc gia.

Tính từ thời điểm Thủ tướng Chính phủ khai trương (ngày 12/3/2019) đến ngày 10/02/2020, đã có hơn 1,26 triệu văn bản điện tử gửi, nhận qua Trục liên thông văn bản quốc gia.

Bên cạnh những kết quả như trên, trong triển khai các nhiệm vụ CPĐT vẫn còn một số tồn tại, hạn chế như chưa hoàn thành các văn bản quy phạm pháp luật làm khung thể chế cho triển khai CPĐT như chưa hoàn hành cơ sở dữ liệu quốc gia về dân cư, đất đai; Trên 70% các bộ, ngành, địa phương chưa có nền tảng tích hợp, chia sẻ dữ liệu; Chưa có nền tảng thanh toán điện tử cho dịch vụ công; Một bộ phận cán bộ, công chức, viên chức chưa có ý thức thay đổi thói quen, vẫn ưu tiên thực hiện theo các phương thức truyền thống.

Nhận định thêm về các kết quả bước đầu trong việc triển khai CPĐT, Bộ trưởng, Chủ nhiệm Văn phòng Chính phủ Mai Tiến Dũng cho biết, các điều kiện kinh doanh và thủ tục hành chính được rà soát và cắt giảm, tiết kiệm được 6.300 tỷ đồng. Việc triển khai gửi nhận văn bản điện tử này đã góp phần giảm đáng kể thời gian gửi, nhận văn bản và giảm các chi phí được 1.200 tỷ đồng.

Hội nghị ghi nhận nhiều ý kiến tham luận về kinh nghiệm triển khai, đánh giá độc lập về CPĐT của các bộ, ngành như Bộ Công Thương, tỉnh An Giang, CMC… cũng như thảo luận về các vấn đề trong việc xây dựng CPĐT.

Link tham khảo: http://antoanthongtin.vn/chinh-tri---xa-hoi/xay-dung-thanh-cong-chinh-phu-dien-tu-bang-suc-manh-noi-tai-105853

## 2. Lỗ hổng Android cho phép gửi phần mềm độc hại qua Bluetooth

Một lỗ hổng trên Android mang tên BlueFrag cho phép kẻ tấn công âm thầm cung cấp phần mềm độc hại và đánh cắp dữ liệu từ các điện thoại gần đó chạy Android 8 Oreo hoặc Android 9 Pie.

Theo Engadget, được phát hiện bởi các nhà nghiên cứu bảo mật tại ERNW, BlueFrag cho phép kẻ xâm nhập chỉ cần biết địa chỉ MAC thiết bị Bluetooth của mục tiêu - đôi khi dễ đoán bằng cách nhìn vào địa chỉ MAC Wi-Fi. ERNW, người dùng thậm chí sẽ không biết cuộc tấn công đang xảy ra.

BlueFrag không hoạt động với Android 10 và có thể chỉ ảnh hưởng đến các phiên bản trước Android 8, tuy nhiên nhóm đã không đánh giá tác động đối với các bản phát hành cũ hơn. Người dùng có thể tự bảo vệ mình bằng cách cài đặt bản vá bảo mật tháng 2.2020 và bản chất lỗ hổng Bluetooth có nghĩa người dùng sẽ phải tương đối gần với kẻ tấn công. Điều này có nghĩa vấn đề sẽ là mối quan tâm trong không gian công cộng.

Một vấn đề đáng quan tâm ở lỗ hổng này là nhiều thiết bị bị ảnh hưởng đã không còn nhận được bản cập nhật phần mềm hoặc chúng không nhận được bản vá một

cách nhất quán. Google chỉ yêu cầu các nhà sản xuất điện thoại phổ biến cung cấp các bản cập nhật bảo mật trong 2 năm và chính sách đó dường như đã được thi hành vào đầu năm 2019. Khi mà Android 8 đã vượt qua mốc 2 năm đó, vì vậy người dùng có thể không bao giờ nhận được bản vá lỗi BlueFrag nếu điện thoại đã quá 2 năm ra mắt.

Ngoài ra, Google cũng cho phép các nhà cung cấp kéo dài đến 90 ngày trước khi vá một lỗ hổng nên lượng thiết bị tổn thương có thể tồn tại trong nhiều tháng.

***Khuyến nghị:*** Người dùng Android cần cập nhật các bản vá mới nhất của thiết bị đang sử dụng phiên bản 8 và 9, ngoài ra với những thiết bị chưa có bản vá chỉ nên bật Bluetooth khi cần để đảm bảo an toàn thông tin.

Link tham khảo: https://thanhnien.vn/cong-nghe/lo-hong-android-cho-phep-gui-phan-mem-doc-hai-qua-bluetooth-1180947.html

### 3. Cảnh giác mất tiền triệu do lừa đảo cước viễn thông quốc tế

Hoạt động lừa đảo cước viễn thông đang bùng phát trở lại. Nếu không cẩn thận và mắc bẫy gọi vào các số máy quốc tế, người dùng di động có thể sẽ bị trừ tài khoản với số tiền lên tới cả triệu đồng.

Chia sẻ với Pv. VietNamNet, đại diện một nhà mạng cho biết, thời gian gần đây, nhà mạng này liên tục nhận được phản ánh của khách hàng về các cuộc gọi lạ. Những cuộc gọi này thường bắt đầu từ các đầu số nước ngoài như: Modova (+373), Tunisia (+216), Equatorial Guinea (+240), Burkina Faso (+226).

Theo nhà mạng trên, thực chất đây là các cuộc gọi nháy máy từ thuê bao nước ngoài đến các thuê bao trong nước, bao gồm cả cuộc gọi nháy máy từ các ứng dụng OTT nhằm mục đích lôi kéo lừa đảo khách hàng gọi lại để phát sinh cước viễn thông ngoài ý muốn.

Những cuộc gọi này thường được thực hiện vào thời điểm buổi tối hoặc trong thời gian nửa đêm về sáng. Đây là lúc đa số người dùng vẫn còn đang ngái ngủ hoặc tưởng người thân gọi về Việt Nam có chuyện cần gấp.

Hầu hết các cuộc gọi được thực hiện với thời lượng vài giây rồi tắt máy. Nếu gọi lại cho các số điện thoại lạ và khi cuộc gọi được kết nối thành công, người nghe chỉ nghe thấy những âm thanh được cài đặt sẵn. Sau đó, tài khoản của họ sẽ lập tức bị trừ những khoản tiền rất lớn.

Để tránh thiệt hại, người dùng nên nên cảnh giác với các cuộc gọi, tin nhắn từ các đầu số lạ quốc tế gọi hoặc nháy máy, nhắn tin vào số điện thoại của mình.

*Một số dấu hiệu nhận biết cuộc gọi, tin nhắn lừa đảo và biện pháp phòng tránh:*

- Các cuộc gọi, tin nhắn Quốc tế về sẽ hiển thị dấu cộng (+) hoặc hoặc 00 ở đầu. Hai số tiếp theo không phải là 84 (Mã nước Việt Nam).

- Các cuộc gọi này xuất hiện hiện dưới dạng nháy máy hoặc có kết nối thời lượng rất ngắn có nội dung thông báo yêu cầu người dùng gọi lại. Với tin nhắn cũng sẽ có nội dung yêu cầu gọi lại.

- Người dùng không thực hiện gọi lại những số máy xuất hiện ở những cuộc gọi nhỡ, gọi đến, tin nhắn có dấu hiện như trên. Chỉ nên gọi đi quốc tế khi biết chắc chắn đó là số điện thoại của người thân ở nước ngoài.

- Các ứng dụng có tính năng thực hiện cuộc gọi thông thường có thông báo mời lựa chọn giữa cuộc gọi có tính phí và cuộc gọi không tính phí. Do vậy, khi thực hiện cuộc gọi bằng các ứng dụng này, người dùng di động nên lưu ý kiểm tra kỹ hình thức thực hiện cuộc gọi đang sử dụng, tránh phát sinh cước ngoài ý muốn.

***Khuyến nghị:*** Người dùng cần cảnh giác với các cuộc gọi nháy máy từ nước ngoài, kiểm tra kỹ thông tin trước khi gọi lại để tránh bị mất tiền cước.

Link tham khảo: https://vietnamnet.vn/vn/cong-nghe/vien-thong/canh-giac-mat-tien-trieu-do-lua-dao-cuoc-vien-thong-quoc-te-613807.html

## TECHNICAL PAGES:

1. Chi tiết về thông tin một số lỗ hổng trên các sản phẩm/dịch vụ phổ biến tại Việt Nam trong tuần, cụ thể như sau:

| STT | Sản phẩm/ dịch vụ | Mã lỗi quốc tế | Mô tả ngắn | Ghi chú |
|---|---|---|---|---|
| 1 | Adobe | CVE-2020-3714<br>CVE-2020-3712<br>CVE-2020-3710<br>… | Nhóm 07 lỗ hổng trên phần mềm Adobe (Adobe Illustrator CC version 24.0,...) cho phép đối tượng chèn và thực thi mã tùy ý.<br>05 lỗ hổng có điểm CVSS: 9,3 (nghiêm trọng). | Đã có thông tin xác nhận và bản vá. |
| 2 | Asus | CVE-2013-3093<br>CVE-2020-7997 | Nhóm 02 lỗ hổng trên sản phẩm của Asus (Asus RT-N56U, Asus WRT-AC66U 3.0.0.4.372_67…) cho phép đối tượng tấn công tấn công tấn công XSS, tấn công CSRF. | Đã có thông tin xác nhận và bản vá |
| 3 | Bitdefender | CVE-2019-17095<br>CVE-2019-17096<br>CVE-2019-17099<br>… | Nhóm 09 lỗ hổng trên một số thành phần của phần mềm Bitdefender (Bitdefender AV for MAC, EPSecurityService.exe,…) cho phép đối tượng tấn công thu thập thông tin, tấn công từ chối dịch vụ. | Đã có thông tin xác nhận và bản vá |
| 4 | Cisco | CVE-2020-3115<br>CVE-2020-3147<br>CVE-2019-16005<br>… | Nhóm 25 lỗ hổng trên sản phẩm của Cisco (Cisco SD-WAN Solution,...) cho phép đối tượng tấn công tấn công chèn và thực thi mã tùy ý, truy cập trái phép vào hệ thống với quyền root, tấn công từ chối dịch vụ | Đã có thông tin xác nhận và bản vá |
| 5 | Apache | CVE-2020-1931<br>CVE-2020-1930<br>CVE-2020-1933<br>… | Nhóm 06 lỗ hổng trên phần mềm Apache (Apache SpamAssassin, Apache Nifi,…) cho phép đối tượng tấn công thu thập thông tin, chèn và thực thi mã tùy ý. | Đã có thông tin xác nhận và bản vá |
| 6 | D-link | CVE-2019-20216<br>CVE-2019-20217 | Nhóm 09 lỗ hổng trên sản phẩm của D-link (DIR-859 | Đã có thông tin |

| | | | | |
|---|---|---|---|---|
| | | CVE-2012-6613<br>… | 1.05 và 1.06B01 Beta01,…) cho phép đối tượng tấn công truy cập hệ thống trái phép, thực thi mã tùy ý.<br>03 lỗ hổng có điểm CVSS: 10,0 (đặc biệt nghiêm trọng). | xác nhận và bản vá |
| 7 | Gitlab | CVE-2019-5464<br>CVE-2019-15585<br>CVE-2019-5470<br>… | Nhóm 18 lỗ hổng trên một số thành phần của Gitlab (Gitlab Community Edition and Enterprise Edition,…) cho phép đối tượng tấn công thu thập thông tin. | Đã có thông tin xác nhận và bản vá |

2. Danh sách IP/tên miền độc hại có nhiều kết nối từ Việt Nam

| **STT** | **Tên miền/IP** |
|---|---|
| 1 | disorderstatus.ru |
| 2 | differentia.ru |
| 3 | atomictrivia.ru |
| 4 | xjpakmdcfuqe.biz |
| 5 | www.cityofangelsmagazine.com |
| 6 | amnsreiuojy.ru |
| 7 | xjpakmdcfuqe.biz |
| 8 | ydbnsrt.me |
| 9 | somicrososoft.ru |
| 10 | xjpakmdcfuqe.in |

3. Các cán bộ kỹ thuật đầu mối về ATTT cần thực hiện:
   - Xử lý các lỗ hổng phát hiện tại bảng 1 (nếu có).
   - Chặn, xử lý các truy nhập tới các tên miền độc hại tại bảng 2.