ỦY BAN NHÂN DÂN **XÃ PHÚ TIẾN**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập – Tự do – Hạnh phúc**
Số: 41 /UBND - VHXH V/v tuyên truyền triển khai thực hiện nhiệm vụ (Đề án 06) trên địa bàn xã Phú Tiến năm 2023	*Phú Tiến, ngày 05 tháng 4 năm 2023*

Kính gửi: - Các Ông, bà trưởng xóm trên địa bàn

Căn cứ Công văn số543/STTTT-TTBCXB, ngày 22/3/2023 của Sở Thông tin và Truyền thông tỉnh Thái Nguyên về việc tuyên truyền triển khai thực hiện nhiệm vụ (Đề án 06) trên địa bàn tỉnh Thái Nguyên năm 2023.

Thực hiện Công văn số 1412/VHTT-TT ngày 30/3/2023 của UBND huyện Định Hóa về việc tiếp tục tuyên truyền triển khai thực hiện nhiệm vụ (Đề án 06) trên địa bàn huyện Định Hóa năm 2023. UBND xã Phú Tiến đề nghị các Ông, bà trưởng xóm trên địa bàn xã triển khai thực hiện một số nội dung sau:

1.Tiếp tục tăng cường công tác thông tin tuyên truyền trên hệ thống loa truyền thanh của xómđể mọi người dân trên địa bàn nâng cao nhận thức về định danh, xác thực điện tử và các Dịch vụ công trực tuyến.

2.Thường xuyên tuyên truyền về 07 phương thức khai thác, sử dụng thông tin công dân trên thẻ Căn cước công dân gắn chip điện tử hoặc trong Cơ sở dữ liệu quốc gia về dân cư thay thế cho việc xuất trình Sổ hộ khẩu, Sổ tạm trú giấy khi thực hiện thủ tục hành chính, Dịch vụ công trực tuyến và sử dụng các dịch vụ, tính năng, tiện ích số của ứng dụng như: Chia sẻ dữ liệu thông qua mã QR định danh, thực hiện thông báo lưu trú…

3. Tuyên truyền tới nhân dân trong xóm đăng nhập vào trang thông tin điện tử của địa phương để xem các tin bài được đăng và đồng thời để đông đảo người dân biết và sử dụng ứng dụng định danh quốc gia trên thiết bị di động (VneID) và cách thức thực hiện các thủ tục hành chính trên Cổng dịch vụ công quốc gia tại địa chỉ: https://dichvucong.gov.vn.

Căn cứ các nội dung nêu trên,UBND xã đề nghị các Ông , bà trưởng xóm tâm triển khai thực hiện./.

Nơi nhận:
- Như trên;
- Lãnh đạo UBND xã;
- Lưu: VP.

TM .ỦY BAN NHÂN DÂN
CHỦ TỊCH

Ngô Tuấn Sơn

PHỤ LỤC: THÔNG TIN LỖ HỔNG BẢO MẬT

(Kèm theo Công văn số: /UBND - VHXH ngày /4/2023 của UBND xã Phú Tiến)

1. Điểm yếu, lỗ hổng tồn tại trên máy tính của các cơ quan, tổ chức, đơn vị trong tháng 02/2023

Trong tháng 02/2023, Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC) phát hiện trên **1.213** điểm yếu, lỗ hổng bảo mật an toàn thông tin tại các hệ thống thông tin của các cơ quan, tổ chức nhà nước, đặc biệt có một số lỗ hổng đã và đang được các nhóm tấn công lợi dụng để thực hiện các cuộc tấn công APT, một số lỗ hổng vẫn còn tồn tại trên nhiều máy của các cơ quan, tổ chức nhà nước chưa được xử lý, cụ thể như sau:

TT	Mã điểm yếu/lỗ hổng	Số lượng máy bị ảnh hưởng	Link tham khảo
1	CVE-2019-0708	**7.780**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2019-0708
2	CVE-2018-20250	**1.600**	https://www.microsoft.com/en-us/security/blog/2019/04/10/analysis-of-a-targeted-attack-exploiting-the-winrar-cve-2018-20250-vulnerability/
3	CVE-2016-6169	**1.534**	https://www.fortiguard.com/zeroday/FG-VD-16-018
4	CVE-2015-5663	**1.478**	http://jvn.jp/en/jp/JVN64636058/index.html
5	CVE-2022-2505	**835**	https://www.mozilla.org/en-US/security/advisories/mfsa2022-28/#CVE-2022-2505

2. Thông tin các lỗ hổng bảo mậttrong các sản phẩm của hãng Microsoft công bố tháng 3/2023

STT	Lỗ hổng bảo mật	Mô tả	Link tham khảo
1	CVE-2023-23397	- Điểm CVSS: 9.1 ***(mức độ ảnh nghiêm trọng)*** - Mô tả: Lỗ hổng trong Microsoft Outlook cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền. Lỗ hổng này đang bị khai thác trong thực tế. - Ảnh hưởng: Microsoft	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23397

		Outlook, Microsoft Office.	
2	CVE-2023-24880	- Điểm CVSS: 5.4 *(mức độ ảnh hưởng trung bình)* - Mô tả: Lỗ hổng trong Windows SmartScreen cho phép đối tượng tấn công thực hiện tấn công vượt qua cơ chế bảo mật (Bypass). Lỗ hổng này đang bị khai thác trong thực tế. - Ảnh hưởng: Windows Server, Windows 10/11.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24880
3	CVE-2023-23392	- Điểm CVSS: 9.8 ***(mức độ ảnh hưởng nghiêm trọng)*** - Mô tả: Lỗ hổng trong HTTP Protocol Stack cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows Server, Windows 11.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23392
4	CVE-2023-23415	- Điểm CVSS: 9.8 ***(mức độ ảnh hưởng nghiêm trọng)*** - Mô tả: Lỗ hổng trong Internet Control Message Protocol (ICMP) cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows Server, Windows 10/11.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23415
5	CVE-2023-23399	- Điểm CVSS: 7.8 ***(mức độ ảnh hưởng cao)*** - Mô tả: Lỗ hổng trong Microsoft Excel cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Office, Microsoft Excel, Microsoft 365.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23399

6	CVE-2023-23400	- Điểm CVSS: 7.2 ***(mức độ ảnh hưởng cao)*** - Mô tả: Lỗ hổng trong Windows DNS Server cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows Server.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23400

3. Khuyến nghị và hướng dẫn khắc phục

- Đề nghị bộ phận chuyên trách về công nghệ thông tin/an toàn thông tin tại các cơ quan, tổ chức, đơn vịphối hợp với các bộ phận có liên quan thực hiện kiểm tra, rà soát, xác định máy tính sử dụng hệ điều hành Windows có khả năng bị ảnh hưởngvà tiến hành cập nhật bản vá kịp thời cho các lỗ hổng bảo mậtnói trên theo hướng dẫn của hãngđể tránh nguy cơ bị tấn công, đặc biệt là các lỗ hổng đã được Bộ Thông tin và Truyền thông, Sở Thông tin và Truyền thông và các cơ quan, đơn vị chức năng cảnh báo *(tham khảo các bản cập nhật phù hợp cho các sản phẩm đang sử dụng tại link nguồn tham khảo tại mục 1, mục 2 của Phụ lục này).*

- Tăng cường giám sát và sẵn sàng phương án xử lý khi phát hiện có dấu hiệu bị khai thác, tấn công mạng; đồng thời thường xuyên theo dõi kênh cảnh báo của các cơ quan chức năng và các tổ chức lớn về an toàn thông tin để phát hiện kịp thời các nguy cơ tấn công mạng.

- Trong trường hợp cần thiết có thể liên hệ đầu mối hỗ trợ của Cục An toàn thông tin: Trung tâm Giám sát an toàn không gian mạng quốc gia, điện thoại 02432091616, thư điện tử: ais@mic.gov.vn.

4. Tài liệu tham khảo

https://msrc.microsoft.com/update-guide
https://www.zerodayinitiative.com/blog/2023/3/14/the-march-2023-security-update-review