

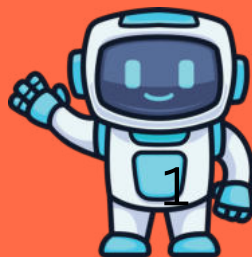


BÌNH DÂN HỌC VỤ SỐ

E-BOOK

Số 5/2025

info





NỘI DUNG

I. KIẾN THỨC, KỸ NĂNG SỐ CƠ BẢN

1. Những hiểm họa phổ biến trong thời đại số hiện nay

2. Người dùng Google Chrome cần cập nhật ngay trình duyệt

3. Hướng dẫn bảo trì và vệ sinh máy tính đúng cách

4. Kỹ năng xử lý khi bị lộ thông tin cá nhân

II. TRAO ĐỔI THẢO LUẬN

5. Hải Phòng ứng dụng trí tuệ nhân tạo, nâng cao hiệu quả công việc tại các cơ quan, đơn vị

6. Chuyển đổi số – Xu thế tất yếu trong quá trình phát triển báo chí hiện đại

7. Chuyển đổi số: Lựa chọn lĩnh vực trọng tâm tạo đột phá

III. HỎI ĐÁP

8. Câu hỏi: Làm thế nào để biết tin nhắn đó là giả mạo ngân hàng?

9. Có nên dùng Wifi công cộng để giao dịch ngân hàng không?

10. Cách phát hiện app lừa đảo trên CH Play/App Store?

I. KIẾN THỨC, KỸ NĂNG SỐ CƠ BẢN

Những hiểm họa phổ biến trong thời đại số hiện nay



1

Lừa đảo qua mạng xã hội

Hình thức: Đối tượng sẽ giả mạo tài khoản người thân, cơ quan nhà nước, ngân hàng, công ty tuyển dụng... nhắn tin xin tiền, lừa nhận thưởng, hoặc thông báo vi phạm pháp luật.

Thủ đoạn: Gửi link giả, yêu cầu chuyển khoản hoặc cung cấp mã OTP, thông tin cá nhân.

Hậu quả: Nếu mọi người làm theo sẽ bị mất tiền, mất quyền truy cập tài khoản, bị lợi dụng danh tính.

Cảnh báo: Mọi người không vội tin vào những tin nhắn, cuộc gọi bất thường, hãy xác minh qua các kênh chính thống hoặc gọi điện trực tiếp cho người thân để xác minh.



2

Tuyên truyền tin giả, thông tin sai lệch

Hình thức: Thông qua mạng xã hội, nhóm chat, ứng dụng nhắn tin... những thông tin, tin đồn thất thiệt về sức khỏe, chính trị, đời tư người nổi tiếng, chính sách xã hội... sẽ được phát tán, lan truyền. Nếu không tỉnh táo kiểm chứng, chúng ta chia sẻ, lan truyền thông tin đó.

Tác hại: Gây hoang mang dư luận, ảnh hưởng đến tâm lý cộng đồng và có thể vi phạm pháp luật nếu chia sẻ, phát tán tin giả.

Cảnh báo: Mọi người chỉ tin và chia sẻ thông tin từ các nguồn chính thống, tập cho mình thói quen luôn kiểm chứng, đối chiếu thông tin từ nhiều nguồn khác nhau trước khi chia sẻ thông tin.



3

Ứng dụng chứa mã độc

Hình thức: Đối tượng lừa đảo sẽ sử dụng các app giả mạo ngân hàng, ví điện tử, app chỉnh sửa ảnh, đoán tuổi, làm đẹp... yêu cầu người dùng cấp quyền truy cập toàn bộ điện thoại.

Tác hại: Đánh cắp thông tin, chiếm quyền kiểm soát thiết bị, theo dõi người dùng, lấy tiền từ tài khoản.

Cảnh báo: Mọi người tuyệt đối không cài ứng dụng không rõ nguồn gốc. Chỉ tải và cài các app từ kho ứng dụng chính thức như CH Play, App Store.



4

Đánh cắp tài khoản cá nhân

Hình thức: Các đối tượng lừa đảo dùng các đường link giả mạo, phần mềm gián điệp, keylogger để lấy cắp tài khoản Facebook, Gmail, Zalo...

Tác hại: Mất quyền kiểm soát tài khoản, bị kẻ gian mạo nhận danh tính, dùng tài khoản để tiếp tục lừa đảo người quen, làm mất uy tín cá nhân cũng như những dữ liệu quan trọng.

Cảnh báo: Mọi người luôn bật xác thực hai bước, tuyệt đối không nhấn vào link lạ, không chia sẻ thông tin đăng nhập cho người khác.



5

Mạo danh cơ quan công quyền để lừa tiền

Hình thức: Các đối tượng lừa đảo sẽ gọi điện giả danh công an, tòa án, viện kiểm sát... thông báo bạn đang bị điều tra, yêu cầu cung cấp thông tin hoặc chuyển tiền để “chứng minh vô tội”.

Dấu hiệu nhận biết: Giọng nói lạnh lùng, dọa dẫm, yêu cầu giữ bí mật, tuyệt đối không chia sẻ với người thân nhằm thao túng tâm lý nạn nhân.

Cảnh báo: Không làm theo những yêu cầu của đối tượng vì không cơ quan chức năng nào làm việc qua điện thoại và yêu cầu chuyển tiền. Mọi người cần bình tĩnh, ngắt cuộc gọi và báo cho các cơ quan chức năng.



6

Lộ dữ liệu cá nhân

Nguyên nhân: Điền thông tin vào website lạ, chụp ảnh, giấy tờ tùy thân lên mạng, chia sẻ mã OTP, mật khẩu cho người lạ...

Tác hại: Bị mạo danh vay tiền, mở tài khoản ngân hàng, nạp tiền điện thoại, bị theo dõi, đánh cắp các thông tin cá nhân.

Cảnh báo: Mọi người cần bảo vệ thông tin cá nhân như bảo vệ tài sản, tuyệt đối không công khai thông tin cá nhân đó lên mạng./.

Người dùng Google Chrome cần cập nhật ngay trình duyệt

Google vừa phát hiện và khắc phục một lỗ hổng bảo mật nghiêm trọng trong trình duyệt Chrome dành cho máy tính để bàn mà người dùng cần cập nhật gấp.

Google cảnh báo rằng lỗ hổng trên trình duyệt Chrome đã bị tin tặc lợi dụng, do đó tất cả người dùng được khuyến cáo nên cập nhật trình duyệt ngay lập tức.

Lỗ hổng bảo mật này nằm trong công cụ JavaScript của Chrome, được gọi là V8, và đã được các chuyên gia bảo mật đánh giá với mức độ nghiêm trọng lên tới 8,8/10. Lỗi này cho phép kẻ tấn công kiểm soát thiết bị của người dùng, từ đó có thể đánh cắp dữ liệu cá nhân hoặc cài đặt phần mềm độc hại chỉ bằng cách khiến người dùng truy cập vào một trang web độc hại được thiết kế đặc biệt.

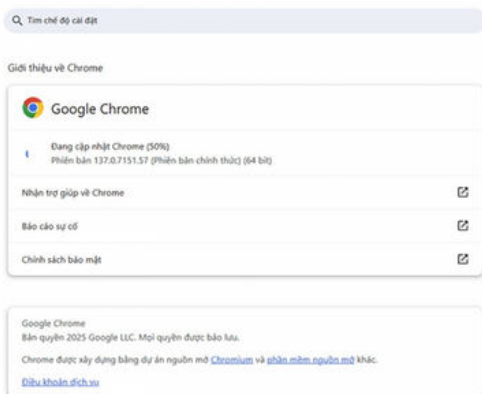
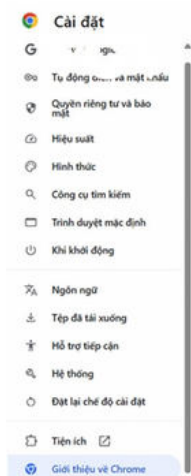
Để khắc phục sự cố, Google đã phát hành bản cập nhật cho Chrome phiên bản 137.0.7151.69, hiện đã có sẵn cho người dùng trên các hệ điều hành Windows, macOS và Linux.

Người dùng Chrome nên làm gì để cập nhật?

Mặc dù Chrome thường tự động cập nhật, Google khuyến nghị người dùng nên kiểm tra thủ công để đảm bảo trình duyệt của họ đã được cập nhật. Để thực hiện điều này, hãy vào menu Chrome, chọn “Trợ giúp” và sau đó là “Giới thiệu về Google Chrome”. Nếu có bản cập nhật, trình duyệt sẽ tự động bắt đầu cài đặt. Người dùng cần nhấp vào “Chạy lại” để hoàn tất quá trình cập nhật.

Google không tiết lộ thời gian lỗ hổng này đã bị khai thác, nhưng công ty xác nhận rằng các kẻ tấn công đang tích cực sử dụng nó. Điều này có nghĩa là những người dùng trì hoãn việc cập nhật có thể gặp rủi ro cao. Việc không cập nhật trình duyệt có thể dẫn đến việc lộ dữ liệu cá nhân.

Để bảo vệ bản thân, người dùng nên kiểm tra phiên bản trình duyệt của mình ngay bây giờ và thực hiện cập nhật mà không chậm trễ. Luôn cập nhật là cách tốt nhất để đảm bảo an toàn cho dữ liệu cá nhân của bản thân./.



Hướng dẫn bảo trì và vệ sinh máy tính đúng cách



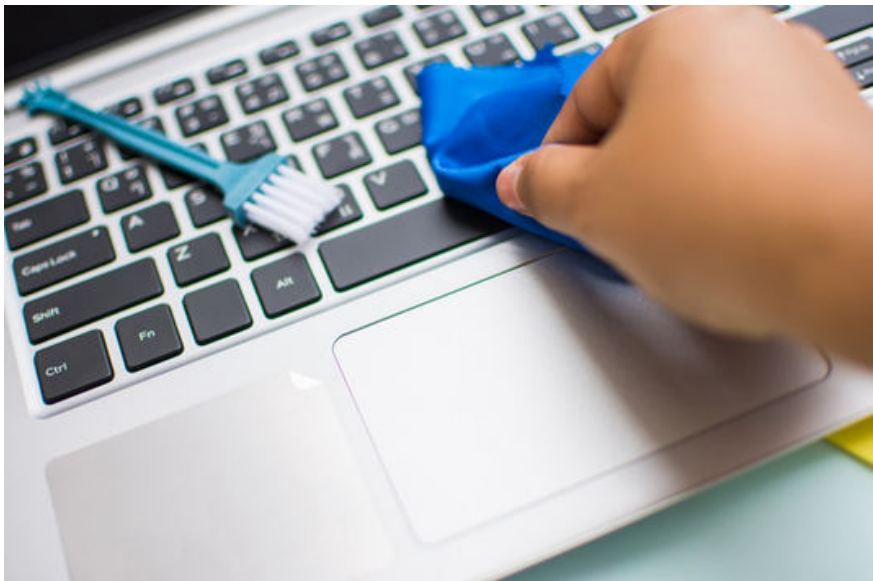
Việc bảo trì và vệ sinh máy tính định kỳ không chỉ kéo dài tuổi thọ thiết bị mà còn duy trì hiệu suất ổn định, đồng thời giảm thiểu nguy cơ hư hỏng do bụi bẩn và nhiệt độ.

Máy tính cá nhân ngày nay đóng vai trò thiết yếu trong đời sống hiện đại, phục vụ đa dạng nhu cầu từ công việc, học tập đến giải trí. Tuy nhiên, không ít người dùng vẫn xem nhẹ việc bảo trì và vệ sinh thiết bị, dẫn đến tình trạng xuống cấp nhanh chóng và hiệu suất suy giảm. Duy trì máy tính trong trạng thái sạch sẽ và được chăm sóc định kỳ không chỉ giúp kéo dài tuổi thọ mà còn đảm bảo hiệu năng hoạt động ổn định và bền bỉ theo thời gian.

Theo ông John Mitchell, chuyên gia công nghệ tại công ty bảo trì thiết bị TechCare (Mỹ), việc vệ sinh và bảo trì máy tính định kỳ giúp loại bỏ bụi bẩn và hạn chế tình trạng quá nhiệt, hai nguyên nhân hàng đầu gây hư hỏng linh kiện bên trong thiết bị.

Ông Mitchell khuyến cáo người dùng nên vệ sinh máy tính định kỳ từ 03 - 06 tháng một lần, tùy theo điều kiện và môi trường sử dụng.

Trước tiên, việc vệ sinh bên ngoài máy tính tuy đơn giản nhưng đòi hỏi sự cẩn trọng. Người dùng nên sử dụng khăn mềm, khô hoặc hơi ẩm để lau màn hình, bàn phím và vỏ máy. Tuyệt đối tránh các loại hóa chất tẩy rửa mạnh, có thể làm trầy xước bề mặt hoặc gây hư hại lớp phủ bảo vệ màn hình.





Đặc biệt, khu vực bàn phím và các khe tản nhiệt cần được làm sạch kỹ bằng bình khí nén hoặc chổi mềm để loại bỏ bụi tích tụ – yếu tố làm cản trở luồng khí, khiến thiết bị dễ nóng lên khi hoạt động.

Đối với phần bên trong máy, ông Mitchell lưu ý: “Nếu không có kinh nghiệm, người dùng nên tìm đến kỹ thuật viên chuyên nghiệp hoặc trung tâm bảo hành để tránh làm hư hại các linh kiện nhạy cảm”.

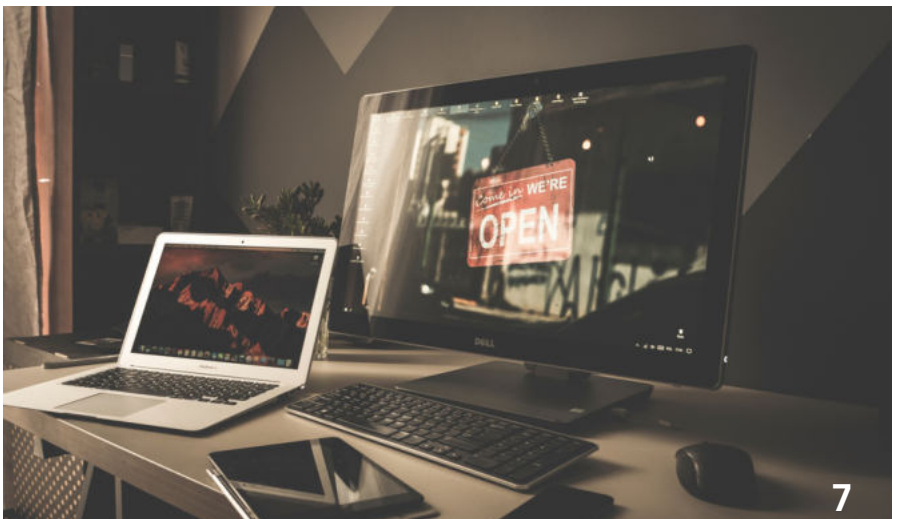
Bụi bẩn tích tụ bên trong có thể gây nghẽn quạt tản nhiệt, khiến máy quá nóng và hiệu năng bị suy giảm rõ rệt. Quá trình vệ sinh nội bộ thường bao gồm việc tháo nắp máy, sử dụng khí nén để làm sạch bụi và kiểm tra tình trạng các bộ phận như quạt làm mát, RAM, ổ cứng.

Bên cạnh vệ sinh phần cứng, bảo trì phần mềm cũng đóng vai trò quan trọng trong việc duy trì hiệu suất máy tính. Người dùng nên thường xuyên cập nhật hệ điều hành, phần mềm diệt virus và dọn dẹp các tập tin rác nhằm tránh tình trạng máy chạy chậm hoặc bị mã độc tấn công.

Ông John Mitchell nhấn mạnh: “Phần mềm được tối ưu hóa sẽ giúp máy tính vận hành trơn tru, đồng thời giảm tải đáng kể cho phần cứng”.

Ngoài ra, một số thói quen sử dụng cũng ảnh hưởng trực tiếp đến độ bền của thiết bị. Người dùng nên tránh đặt máy gần nguồn nhiệt, hạn chế va đập, sử dụng nguồn điện ổn định và thực hiện sao lưu dữ liệu định kỳ. Đây đều là những biện pháp đơn giản nhưng hiệu quả, giúp máy tính vận hành bền bỉ và an toàn trong thời gian dài.

Việc bảo trì và vệ sinh máy tính không đơn thuần là thao tác kỹ thuật, mà còn là cách người dùng thể hiện sự chủ động trong việc gìn giữ và kéo dài tuổi thọ thiết bị. Đầu tư thời gian và công sức vào công việc này sẽ giúp người dùng hạn chế rủi ro, tiết kiệm chi phí sửa chữa và nâng cao trải nghiệm công nghệ mỗi ngày./



Kỹ năng xử lý khi bị lộ thông tin cá nhân



Trong môi trường số, việc để lộ thông tin cá nhân như số căn cước công dân (CCCD), mật khẩu tài khoản mạng xã hội, email, tài khoản ngân hàng, số điện thoại...có thể dẫn đến nhiều rủi ro nghiêm trọng như: Bị mạo danh vay tiền, đánh cắp tài khoản, chiếm đoạt tài sản hoặc phát tán thông tin riêng tư. Vì vậy, khi phát hiện hoặc nghi ngờ bị lộ thông tin, bạn cần cần bình tĩnh và xử lý theo 5 bước sau:

Bước 1: Đổi ngay mật khẩu tất cả các tài khoản liên quan

- Ưu tiên đổi mật khẩu tài khoản email, ngân hàng, mạng xã hội, dịch vụ công, tài khoản lưu trữ đám mây (Google Drive, iCloud...).
- Sử dụng mật khẩu mạnh (kết hợp chữ, số, ký tự đặc biệt) và không lặp lại mật khẩu cũ.



Bước 2: Kiểm tra thiết bị và gỡ bỏ ứng dụng lạ.

- Quét virus toàn bộ điện thoại/máy tính bằng phần mềm uy tín như Kaspersky, Avast, Bitdefender..
- Gỡ bỏ các ứng dụng lạ, App yêu cầu quyền truy cập sâu (truy cập camera, danh bạ, tin nhắn...).
- Tắt quyền truy cập không cần thiết đối với các ứng dụng đang dùng.



Bước 3: Kích hoạt bảo mật hai lớp (2FA).

- Bật xác minh 2 bước cho các tài khoản chính (email, Facebook, Zalo, ngân hàng điện tử...).
- Dùng ứng dụng xác thực (Google Authenticator, Microsoft Authenticator) thay vì chỉ dùng SMS OTP để tăng độ an toàn.



Bước 4: Báo cáo và khóa tạm thời tài khoản bị chiếm đoạt

- Nếu mất quyền kiểm soát tài khoản (Facebook, Zalo...), cần báo cáo lên nền tảng đó để khóa tài khoản khẩn cấp.
- Với ngân hàng, gọi tổng đài để yêu cầu khóa tài khoản, thẻ hoặc phong tỏa giao dịch đáng ngờ.
- Với email, nếu không thể đăng nhập, dùng chế độ “Quên mật khẩu” để khôi phục bằng số điện thoại hoặc email phụ.

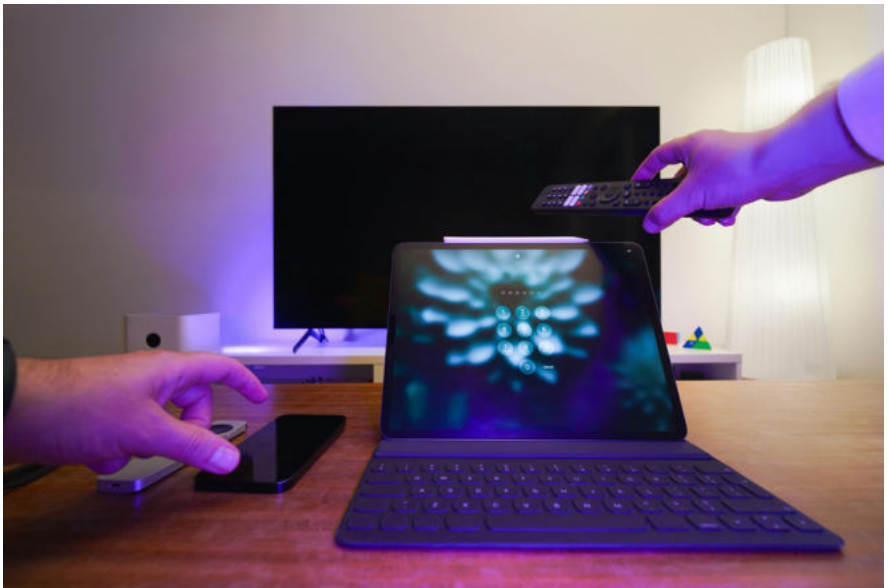


Bước 5: Thông báo tới cơ quan chức năng và gửi thông báo tới những người thân, quen

- Gửi phản ánh tới:
 - + Tổng đài 156 (Bộ Khoa học và Công nghệ), báo cáo tin nhắn lừa đảo, giả mạo.
 - + Số điện thoại đường dây nóng 0692.345.860 của Cục Cảnh sát Hình sự (Bộ Công an) là đầu mối tiếp nhận tin báo, tố giác của người dân về các vụ lừa đảo chiếm đoạt tài sản hoặc công an địa phương nơi mình sinh sống.
 - + Đăng bài cảnh báo người thân, bạn bè nếu tài khoản bị chiếm để tránh kẻ gian tiếp tục lừa đảo.

*** Lưu ý:**

- Nếu nghi bị lộ mật khẩu qua ứng dụng độc hại, cần đổi trên một thiết bị sạch (đã quét virus).
- Tuyệt đối không cung cấp mã OTP, ảnh CCCD, mật khẩu cho bất kỳ ai qua mạng, kể cả người xưng là công an, ngân hàng.
- Luôn kiểm tra kỹ nguồn tin, đường link, ứng dụng trước khi truy cập.
- Cập nhật phần mềm thường xuyên để tránh lỗ hổng bảo mật./.





II. TRAO ĐỔI, THẢO LUẬN

Hải Phòng ứng dụng trí tuệ nhân tạo, nâng cao hiệu quả công việc tại các cơ quan, đơn vị

Thực hiện Nghị quyết số 57-NQ/TW của Bộ Chính trị về đột phá phát triển khoa học công nghệ, đổi mới sáng tạo và chuyển đổi số quốc gia, thời gian qua, thành phố Hải Phòng đã tích cực đẩy mạnh xây dựng chính quyền điện tử, hướng tới chính quyền số với nhiều giải pháp thiết thực, đồng bộ.

Theo đó, việc ứng dụng trí tuệ nhân tạo (AI) vào công tác quản lý, điều hành và phục vụ người dân được thành phố xác định là một trong những nhiệm vụ trọng tâm nhằm nâng cao hiệu quả hoạt động của bộ máy chính quyền.

Từ tháng 4/2025, Công ty Cổ phần Công nghệ HeyU đã phối hợp với Sở Khoa học và Công nghệ thành phố Hải Phòng triển khai thí điểm ứng dụng công nghệ “AI Hải Phòng” tại một số cơ quan, đơn vị trên địa bàn.

Sau một tháng tập huấn và đưa vào sử dụng thử nghiệm tại 8 đơn vị, gồm Ủy ban nhân dân quận Hải An, huyện Kiến Thụy, quận Lê Chân, Sở Khoa học và Công nghệ, Sở Tư pháp, Hội Chữ thập đỏ thành phố, Liên hiệp hội khoa học kỹ thuật thành phố và Trung tâm Báo chí và Truyền thông thành phố với sự tham gia của gần 800 cán bộ, công chức, viên chức, hệ thống đã bước đầu mang lại những kết quả tích cực.

Theo báo cáo của Sở Khoa học và Công nghệ Hải Phòng, ứng dụng “AI Hải Phòng” đã tự động hóa khoảng 80% các công việc hành chính như soạn thảo văn bản, lập báo cáo, tra cứu dữ liệu, viết bài phát biểu, gửi email... góp phần giảm tải áp lực công việc, tinh gọn quy trình, đồng bộ thông tin và nâng cao hiệu quả công tác quản lý, điều hành.





Đặc biệt, đối với lãnh đạo các cấp, AI đóng vai trò như một “trợ lý thông minh”, giúp tổng hợp tin tức, phát hiện thông tin sai lệch, phân tích dữ liệu và đề xuất phương án xử lý truyền thông, hỗ trợ đưa ra các quyết định chính xác, kịp thời.

Hệ thống ứng dụng được triển khai theo mô hình riêng biệt (Private AI), dữ liệu được xử lý bằng các mô hình ngôn ngữ huấn luyện nội bộ, chạy trên máy chủ riêng đặt tại Việt Nam, tuân thủ đầy đủ các quy định của Luật An ninh mạng và Nghị định số 117/2021/NĐ-CP về quản lý dữ liệu. Điều này giúp bảo đảm an toàn, bảo mật thông tin, đồng thời tận dụng hiệu quả nguồn dữ liệu mở và dữ liệu dùng chung của thành phố.

Bên cạnh vai trò trợ lý cho lãnh đạo, ứng dụng “AI Hải Phòng” còn phát triển nhiều tính năng hữu ích cho cán bộ, công chức, viên chức. Hệ thống có thể tự động lập báo cáo, kế hoạch công tác, tóm tắt văn bản, tra cứu nhanh hồ sơ, tương tác trực tiếp với tài liệu, thậm chí soạn thảo bài phát biểu phù hợp với từng sự kiện, hoàn cảnh cụ thể. Trợ lý AI giúp cán bộ nhanh chóng tạo ra các văn bản hành chính đúng chuẩn, tiết kiệm thời gian và giảm thiểu sai sót do yếu tố con người.

Ngoài ra, ứng dụng còn tích hợp khả năng cá nhân hóa công việc, hỗ trợ cán bộ theo dõi tiến độ nhiệm vụ, quản lý hồ sơ công việc cá nhân, nhắc lịch họp, lịch trình một cách linh hoạt, chính xác, thông qua các thông báo trực tiếp gửi đến thiết bị di động.

Với những tính năng vượt trội, hệ thống trợ lý AI giúp rút ngắn đáng kể thời gian thực hiện nhiệm vụ, từ việc lập báo cáo, soạn thảo văn bản đến tra cứu dữ liệu, đồng thời nâng cao chất lượng, tính chính xác trong công việc hành chính.

Sau quá trình tập huấn thử nghiệm, Sở Khoa học và Công nghệ Hải Phòng sẽ tiếp tục phối hợp Công ty Cổ phần Công nghệ HeyU hoàn thiện, bổ sung các tính năng, mở rộng triển khai ứng dụng phục vụ đồng thời cán bộ, công chức và người dân.

Thành phố Hải Phòng phấn đấu trở thành địa phương đi đầu cả nước trong việc ứng dụng AI vào công tác quản lý, điều hành và phục vụ người dân, góp phần xây dựng chính quyền số, đô thị thông minh, vì sự phát triển bền vững./.





Chuyển đổi số - Xu thế tất yếu trong quá trình phát triển báo chí hiện đại

Trong bối cảnh thế giới đang bước vào cuộc cách mạng công nghiệp 4.0, thời đại mà tốc độ trở thành tiêu chuẩn mới của hiệu quả. Chuyển đổi số không còn là một lựa chọn, mà là con đường tất yếu mọi lĩnh vực tồn tại và phát triển. Đối với báo chí, đặc biệt là báo chí địa phương như Hải Phòng, chuyển đổi số là một hành trình đầy thách thức nhưng cũng mở ra cơ hội bứt phá mạnh mẽ, nếu chúng ta biết tận dụng đúng mọi nguồn lực.

1. Chuyển đổi số báo chí: Không chỉ là công nghệ, mà là cuộc cách mạng tư duy

Chuyển đổi số báo chí không đơn thuần là số hóa nội dung hay đăng báo lên các nền tảng kỹ thuật số. Bản chất của nó là quá trình tái cơ cấu toàn diện từ tư duy làm báo, quy trình sản xuất, tác nghiệp, phân phối thông tin đến mô hình quản trị và cách tiếp cận bạn đọc. Báo chí số đòi hỏi một hệ sinh thái mới, nơi công nghệ là nền tảng, dữ liệu là nhiên liệu, còn con người là trung tâm sáng tạo và thích ứng.

Chuyển đổi số trong lĩnh vực báo chí thực chất là một cuộc cách mạng văn hóa trong mỗi tòa soạn. Nó đòi hỏi sự thay đổi từ bên trong: Từ thói quen làm báo truyền thống sang tư duy mở, linh hoạt, cá nhân hóa nội dung theo hành vi người dùng; từ mô hình quản lý tập trung sang môi trường làm việc kết nối, phi tuyến tính; từ thái độ phòng thủ sang chủ động thích ứng và sáng tạo. Như T. Siebel từng chỉ ra, quá trình này mang tính “đứt gãy”, nó không cho phép chúng ta “lột xác” nửa vời. Ai không thay đổi, sẽ bị thay thế. Báo chí Hải Phòng cũng cần nhanh chóng vượt qua “bi kịch đổi mới” để bước ra khỏi vùng an toàn, từ bỏ những thói quen cũ, hướng tới một mô hình báo chí linh hoạt, tương tác và đa nền tảng.





2. Những thách thức, rào cản cần phải vượt qua

Chúng ta phải thẳng thắn thừa nhận rằng không ít cơ quan báo chí còn đang loay hoay trong quá trình chuyển đổi. Rào cản không nằm ở công nghệ bởi công nghệ có thể mua. Rào cản lớn nhất là con người, là văn hóa cũ, là tư duy đóng kín. Khi tổ chức vẫn tồn tại tâm lý e ngại thay đổi, tự mãn với thành quả cũ, hoặc vận hành theo mô hình “lãnh đạo là trung tâm”, thì công nghệ dù hiện đại cũng khó phát huy hiệu quả. Nhiều tòa soạn còn thiếu chiến lược tổng thể, thiếu đội ngũ “nhà báo số” có kỹ năng đa phương tiện, và chưa xác lập được văn hóa tổ chức lấy đổi mới làm gốc rễ.

Tư duy lãnh đạo theo kiểu “lãnh đạo là trung tâm” khiến cho bộ máy ì ạch, kém linh hoạt. Văn hóa cục bộ, lợi ích nhóm khiến tòa soạn khó đổi mới, dễ xảy ra tình trạng “dư người thiếu việc – thừa quy trình thiếu sáng tạo”. Tâm lý sợ hãi trước cái mới, ngại học, ngại thay đổi càng khiến tiến trình chuyển đổi số trở nên lạc nhịp.

Nhiều nhà báo vẫn chưa được đào tạo bài bản về kỹ năng số, chưa quen với các công cụ hiện đại như AI, Big Data, quản trị CMS – Hệ thống quản lý nội dung tích hợp hay tối ưu hóa SEO – quá trình tối ưu hóa website, dù đây là những kỹ năng căn bản trong môi trường báo chí số hiện nay.





3. Giải pháp để thích ứng với xu thế tất yếu trong quá trình phát triển báo chí hiện đại

Để thích ứng với xu thế tất yếu trong quá trình phát triển báo chí hiện đại, điều kiện tiên quyết là chuyển đổi tư duy lãnh đạo. Lãnh đạo các cơ quan báo chí cần là người “mở khóa” cho tổ chức, là dám đặt lại câu hỏi: “Chúng ta đang ở đâu – muốn đi đâu – bằng cách nào?”, và quan trọng nhất: “Giá phải trả là gì?”

Chuyển đổi số không thể thành công nếu thiếu chiến lược rõ ràng và hành động bài bản. Cần giải quyết những bài toán với những yếu tố nền tảng sau:
Về chiến lược: Cần xây dựng chiến lược số hóa phù hợp với đặc thù từng tòa soạn.

Về công nghệ: Xây dựng kiến trúc công nghệ mở, ứng dụng tòa soạn điện tử tích hợp, triển khai CMS, tích hợp trí tuệ nhân tạo để gợi ý nội dung, phân tích hành vi bạn đọc, cải thiện trải nghiệm người dùng.

Về con người: Xây dựng các chương trình đào tạo chuyên sâu cho đội ngũ phóng viên, biên tập viên, kỹ thuật viên về năng lực số, kỹ năng tác nghiệp đa phương tiện, làm báo dữ liệu, phân tích tương tác. Khuyến khích tinh thần dám nghĩ, dám làm, dám thất bại để tiến bộ.

Về mô hình tổ chức: Xây dựng văn hóa tổ chức mở, linh hoạt, thúc đẩy hợp tác – chia sẻ – sáng tạo. Chuyển từ mô hình “quản trị theo mệnh lệnh” sang “quản trị theo năng lực và dữ liệu”, tăng quyền tự chủ cho nhóm sản xuất nội dung, khuyến khích phản biện và đổi mới sáng tạo.

Về xây dựng văn hóa đổi mới, học tập liên tục: Mỗi tòa soạn cần trở thành “trường học số”, nơi mà mọi thành viên không ngừng cập nhật tri thức và kỹ năng.

Tuy nhiên, chuyển đổi số bền vững không thể dựa vào công nghệ một cách mù quáng. Cốt lõi vẫn là con người, là năng lực đổi mới, khả năng học hỏi và tinh thần trách nhiệm của đội ngũ.





Sự phát triển bền vững phải là sự phát triển thật, chất lượng thật, nội dung thật, giá trị thật. Báo chí phải hướng đến việc phục vụ cộng đồng, nâng cao dân trí, bảo vệ cái đúng, cái đẹp trong xã hội. Muốn vậy, chúng ta cần một nền báo chí tỉnh táo trước các xu hướng “ngáo công nghệ”, không chạy theo các lượt like ảo, mà gắn với sứ mệnh cốt lõi của mình: trung thực, nhân văn, khách quan và kịp thời.

Bài học từ các đơn vị tiên phong như Tuổi Trẻ, VietnamPlus hay VnExpress cho thấy, thành công không đến từ những “bước nhảy vọt về công nghệ”, mà từ sự thay đổi đồng bộ và bền bỉ, nơi mọi người trong tổ chức đều cùng chuyển đổi.

Quá trình chuyển đổi số sẽ không có điểm kết thúc. Đó là một hành trình liên tục thích ứng, liên tục học hỏi, liên tục đổi mới, nơi cần sự chung tay của tất cả: Từ lãnh đạo đến mỗi phóng viên, từ cơ quan quản lý đến doanh nghiệp công nghệ. Hãy nhớ: tốc độ không quyết định tất cả, nhưng trong kỷ nguyên số, thiếu tốc độ thì mọi nỗ lực sẽ trở nên vô nghĩa. Và trong hành trình ấy, nếu không thay đổi, chúng ta sẽ bị thay thế.

Hải Phòng, với tinh thần thành phố Cảng kiên cường có đầy đủ điều kiện để trở thành địa phương tiên phong trong chuyển đổi số báo chí. Nhưng điều đó chỉ thành hiện thực khi chúng ta đồng lòng hành động, sẵn sàng vượt qua những giới hạn cũ, dám nghĩ lớn, làm thật và làm đến cùng./.





Chuyển đổi số: Lựa chọn lĩnh vực trọng tâm tạo đột phá

Xác định chuyển đổi số là nhiệm vụ trọng tâm hàng đầu, Hải Phòng quyết liệt trong công tác lãnh đạo, chỉ đạo triển khai và ưu tiên nguồn lực thực hiện. Nhờ đó, thành phố đã đạt được những kết quả rất cụ thể, tạo động lực và mở ra cơ hội mới cho sự phát triển kinh tế – xã hội. Trên cơ sở này, Hải Phòng tiếp tục lựa chọn những lĩnh vực thế mạnh, ưu tiên đầu tư triển khai có trọng tâm nhằm tạo giá trị rõ nét, thúc đẩy tăng trưởng.

Chuyển biến đồng bộ, rõ nét

Xuyên suốt từ năm 2022 đến nay, Hải Phòng luôn xác định đẩy mạnh chuyển đổi số là một trong những mục tiêu trọng tâm trong chủ đề và định hướng hoạt động hằng năm, để các cấp, ngành, địa phương tập trung thực hiện. Trong năm 2025, cùng với các mục tiêu như mở rộng không gian kinh tế, đô thị, hoàn thiện cơ chế chính sách đặc thù, chuyển đổi số tiếp tục là một trong những nội dung quan trọng được Thành ủy, Hội đồng nhân dân (HĐND) và Ủy ban nhân dân (UBND) thành phố xác định, với nhiều giải pháp cụ thể nhằm tạo chuyển biến thực chất và mạnh mẽ hơn.



Mạng 5G đang được phổ biến trên địa bàn thành phố



Theo Phó chủ tịch UBND thành phố Hoàng Minh Cường, xác định chuyển đổi số là nhiệm vụ trọng tâm hàng đầu, thành phố tập trung chỉ đạo quyết liệt, đồng thời ưu tiên nguồn lực để thực hiện các chỉ tiêu, nhiệm vụ quan trọng theo Nghị quyết số 03 của Ban Thường vụ Thành ủy về “Chuyển đổi số thành phố Hải Phòng đến năm 2025, định hướng đến năm 2030”. Cụ thể, năm 2022, thành phố phân bổ 169 tỷ đồng thực hiện 62 nhiệm vụ; năm 2023 bố trí 350 tỷ đồng cho 75 nhiệm vụ; năm 2024 bố trí 300 tỷ đồng thực hiện 81 nhiệm vụ; năm 2025 dự kiến phân bổ 246 tỷ đồng cho 79 nhiệm vụ.

Nhờ vậy, mặc dù “khởi động” chậm hơn một số địa phương, nhưng chuyển đổi số tại Hải Phòng được triển khai đồng bộ, đạt những kết quả bước đầu rõ nét, mở ra các cơ hội phát triển mới. Điểm nhấn nổi bật là Dự án Chính quyền số của thành phố được đưa vào vận hành và khai thác, đánh dấu bước chuyển quan trọng trong quá trình chuyển đổi số, hỗ trợ tích cực công tác chỉ đạo, điều hành của các cơ quan chính quyền cũng như cung cấp dữ liệu, dịch vụ số phục vụ người dân và doanh nghiệp.

Việc phát triển dữ liệu số, nền tảng số được chú trọng, được xem là nguồn tài nguyên tạo ra dư địa phát triển mới. Kho dữ liệu dùng chung đang được tích cực cập nhật, làm đầy, với 264 bộ dữ liệu, 2.767 trường thông tin, hơn 504.717 bản ghi dữ liệu. Các ứng dụng số từ đó được đưa vào sử dụng như những công cụ tiện ích, giúp người dân trải nghiệm, khai thác và sử dụng hiệu quả dữ liệu.



Cảng biển, logistics là những lĩnh vực ưu tiên chuyển đổi số nhằm tạo đột phá trong thời gian tới



Tính đến nay, 100% số xã, phường, thị trấn trên địa bàn thành phố có mạng Internet băng rộng cáp quang, không còn vùng lõm sóng. Mạng 5G phủ sóng tại khu vực trung tâm thành phố, cảng biển, khu công nghiệp và trung tâm thương mại. Hạ tầng trung tâm dữ liệu điện toán đám mây được hoàn thiện. 100% số thủ tục hành chính đủ điều kiện được cung cấp trực tuyến toàn trình, nâng tỷ lệ dịch vụ công trực tuyến toàn trình từ 28% lên 69,5%.

Ưu tiên khu vực cảng biển, khu công nghiệp và logistics

Bên cạnh những kết quả đạt được, công cuộc chuyển đổi số của thành phố còn một số hạn chế như: chưa có trung tâm dữ liệu lớn, cáp quang biển, trạm mặt đất vệ tinh; thiếu dữ liệu số và nhân lực số; chưa có mô hình đô thị thông minh hiệu quả. Tỷ lệ kinh tế số trong một số ngành, lĩnh vực và hoạt động thương mại điện tử còn thấp. Thành phố lựa chọn 5 lĩnh vực mũi nhọn (y tế, giáo dục, xây dựng, giao thông và tài nguyên môi trường) để ưu tiên chuyển đổi số nhưng chưa thực sự tạo được dấu ấn rõ rệt.

Tại cuộc họp đánh giá kết quả thực hiện Nghị quyết số 03 của Ban Thường vụ Thành ủy, đồng chí Bí thư Thành ủy Lê Tiến Châu yêu cầu khẩn trương rà soát các chỉ tiêu, nhiệm vụ chuyển đổi số, bảo đảm đạt bằng hoặc cao hơn mức Trung ương đề ra. Đồng chí nhấn mạnh, thay vì đầu tư dàn trải, thành phố cần lựa chọn 3 lĩnh vực trọng tâm, có thể mạnh là cảng biển, khu công nghiệp và logistics để tập trung nguồn lực đầu tư, tạo chuyển biến nổi bật, phát huy giá trị và thúc đẩy tăng trưởng. Trong đó, thành phố định hướng xây dựng các khu công nghiệp trở thành khu vực đổi mới sáng tạo; ưu tiên đầu tư hạ tầng số cho cả khu công nghiệp và cảng biển; đồng thời tập trung thu hút nhân lực chất lượng cao phục vụ chuyển đổi số, thông qua các chính sách đãi ngộ về đào tạo, nhà ở...

Ngoài 3 lĩnh vực trọng tâm nêu trên, với chủ trương hợp nhất tỉnh Hải Dương và thành phố Hải Phòng, công tác chuyển đổi số càng đặt ra những yêu cầu mới, đặc biệt trong xây dựng chính quyền số, nhằm hỗ trợ hiệu quả công tác lãnh đạo, điều hành.

Với tinh thần đổi mới mạnh mẽ, dám nghĩ, dám làm, luôn đi đầu và sáng tạo trong thực hiện nhiệm vụ, Hải Phòng quyết tâm thực hiện thành công công cuộc chuyển đổi số, tạo động lực quan trọng để hiện thực hóa khát vọng vươn mình trong kỷ nguyên mới./.



III. HỎI ĐÁP

Làm thế nào để biết tin nhắn đó là giả mạo ngân hàng?

Trả lời: Để nhận biết một tin nhắn giả mạo ngân hàng, có thể dựa vào những dấu hiệu sau đây:

1, Tin nhắn dùng ngôn ngữ bất thường: Nếu tin nhắn bạn nhận được có nhiều lỗi chính tả, cách diễn đạt lủng củng, xưng hô không đúng với phong cách chuyên nghiệp thường thấy của ngân hàng, rất có thể đó là tin giả mạo.

2, Yêu cầu cung cấp thông tin cá nhân: Ngân hàng không bao giờ yêu cầu người sử dụng dịch vụ cấp mật khẩu, mã OTP, số thẻ, mã PIN hay bất kỳ thông tin bảo mật nào qua tin nhắn hoặc cuộc gọi. Nếu nhận được yêu cầu như vậy, mọi người cần cảnh giác cao độ.

3, Gửi kèm đường link lạ: Tin nhắn lừa đảo thường đính kèm đường link giả mạo có tên gần giống với website ngân hàng, nhưng khác một vài ký tự. Khi bấm vào, bạn có thể bị dẫn đến trang web giả để đánh cắp thông tin.

4, Nội dung tin nhắn gây hoang mang hoặc quá hấp dẫn: Tin nhắn có thể dọa người dùng với những nội dung như “tài khoản sắp bị khóa”, “có giao dịch bất thường”, hoặc là “bạn đã trúng thưởng lớn”. Mục đích là khiến người dùng hoang mang hoặc mừng rỡ mà vội vàng làm theo hướng dẫn.

5, Tin nhắn gửi từ số điện thoại lạ: Tin nhắn chính thức của ngân hàng thường hiển thị tên thương hiệu (ví dụ: Vietcombank, BIDV...), còn tin nhắn giả thường đến từ các số điện thoại di động không rõ ràng.

Bạn cần làm gì nếu nhận được những tín nhắn như trên?

- Tuyệt đối không bấm vào đường link lạ, không cung cấp bất kỳ thông tin nào.

- Không gọi lại hoặc trả lời những số điện thoại khả nghi.

- Nếu nghi ngờ, hãy gọi trực tiếp đến tổng đài chính thức của ngân hàng (số in trên mặt sau thẻ ATM hoặc trên website chính thức) để kiểm tra.

Việc cẩn trọng với từng tin nhắn sẽ giúp bạn bảo vệ tài khoản và tài sản của mình an toàn trước các thủ đoạn lừa đảo ngày càng tinh vi hiện nay.



Có nên dùng Wifi công cộng để giao dịch ngân hàng không?

Bạn không nên dùng wifi công cộng (quán cà phê, sân bay, trung tâm thương mại...) để truy cập ứng dụng hoặc website ngân hàng vì tiềm ẩn rủi ro rất cao vì những lý do sau đây:

1, Wifi công cộng dễ bị tin tặc theo dõi: Tin tặc có thể cài thiết bị hoặc phần mềm theo dõi trên mạng wifi công cộng để đánh cắp thông tin mà bạn nhập vào – như tên đăng nhập, mật khẩu, mã OTP...

2, Bạn không kiểm soát được độ an toàn của mạng: Wifi công cộng thường không có lớp bảo mật cao, ai cũng có thể truy cập, thậm chí hacker có thể lập ra mạng wifi giả mạo có tên gần giống để đánh lừa người dùng.

3, Thông tin tài khoản ngân hàng là dữ liệu nhạy cảm: Chỉ cần một sơ suất nhỏ, bạn có thể bị mất tiền trong tài khoản hoặc bị lợi dụng để thực hiện các giao dịch trái phép.

Chính vì những lý do trên, cách tốt nhất là bạn chỉ nên thực hiện giao dịch ngân hàng khi:

Dùng mạng di động 4G/5G cá nhân hoặc wifi tại nhà hoặc cơ quan (có độ an toàn cao hơn).

Luôn kiểm tra kỹ địa chỉ website ngân hàng trước khi đăng nhập, và cài ứng dụng chính thức từ kho ứng dụng uy tín (App Store, CH Play).





Cách phát hiện app lừa đảo trên CH Play/App Store?

Mặc dù CH Play (Android) và App Store (iOS) đều có cơ chế kiểm duyệt ứng dụng, nhưng vẫn có một số app lừa đảo lọt qua được. Để tránh tải nhầm ứng dụng giả mạo, bạn nên chú ý các dấu hiệu sau:

1, Tên ứng dụng giống nhưng không hoàn toàn trùng khớp: App giả mạo thường có tên gần giống ứng dụng thật, như thêm dấu, thêm ký tự lạ hoặc viết sai chính tả (ví dụ: “Vietcombankk”). Vì vậy bạn cần kiểm tra kỹ tên trước khi cài đặt.

2, Nhà phát hành không phải chính thức: Ứng dụng ngân hàng hoặc công ty lớn luôn có nhà phát hành rõ ràng (ví dụ: Ngân hàng TMCP Vietcombank). Nếu thấy nhà phát hành lạ, không rõ nguồn gốc, bạn nên kiểm tra cẩn thận.

3, Lượt tải về và đánh giá thấp:

App uy tín thường có lượt tải rất cao (từ hàng trăm nghìn đến hàng triệu lượt), nhiều đánh giá tích cực.

App lừa đảo thường có ít lượt tải, nhiều đánh giá 1 sao, hoặc bình luận phản ánh bị lừa. Chính vì vậy bạn hãy đọc bình luận người dùng trước khi cài đặt.

4, Biểu tượng (icon) khác thường: Ứng dụng giả có thể dùng logo mờ, lệch, màu sắc khác bản chính. Chính vì vậy, nếu bạn nhận thấy biểu tượng không quen thuộc, đừng tải vội về.

5, Yêu cầu quyền truy cập bất thường: Nếu một app ngân hàng nhưng lại đòi quyền truy cập camera, danh bạ, vị trí, micro... một cách bất hợp lý, có thể là app giả đang cố đánh cắp thông tin. Nếu rơi vào trường hợp này bạn nên từ chối và gỡ bỏ ngay ứng dụng.

Lưu ý

- Chỉ tải ứng dụng từ các nguồn chính thức như:

+ Trang web chính thức của ngân hàng, tổ chức.

+ Đường link giới thiệu từ website có uy tín.

- Không tìm app bằng cách tự gõ tên trên kho ứng dụng, vì dễ nhầm lẫn với app giả mạo.

- Khi nghi ngờ, bạn hãy hỏi tổng đài hoặc tra cứu từ trang chủ chính thức trước khi tải, cài đặt.

Việc giữ thói quen kiểm tra kỹ trước khi cài app sẽ giúp bạn tránh mất tiền, mất dữ liệu, và bị lừa đảo qua điện thoại./.