# Truy cập Internet bảo đảm an toàn đối với công chức, viên chức Kho bạc Nhà nước

NGUYỄN THỊ HỒNG YẾN

Trong thời gian qua, để bảo đảm an toàn thông tin cho toàn hệ thống KBNN, KBNN đã chỉ đạo KBNN các tỉnh, thành phố phân công công chức trực giám sát, hỗ trợ, ứng cứu và khắc phục sự cố an toàn thông tin. Bên cạnh đó, công chức, viên chức KBNN cần nâng cao cảnh giác, đảm bảo an toàn an ninh mạng trong quá trình sử dụng các hệ thống CNTT của KBNN, trong đó đặc biệt là các thao tác liên quan đến truy cập internet cần đảm bảo an toàn mọi nơi, mọi lúc.

*Từ khóa: An ninh, an toàn mạng*

*Over the past years, to ensure the information security for all State Treasury offices, the Central State Treasury has provided leadership to provincial Treasury offices to assign officials on duty for monitoring, supporting, and troubleshooting any incidents in information security. In addition, all Treasury officials should be more cautious in ensuring information security during their use of State Treasury's IT systems, especially the operations related to the access to the Internet should be secured anytime and anywhere.*

*Tag: Security, cyber security*

Theo khuyến nghị của tổ chức Liên minh an ninh mạng quốc gia để truy cập internet an toàn, người sử dụng (NSD) cần cân nhắc những lưu ý sau: Khi ngày càng có nhiều dạng mã độc, virus máy tính nguy hiểm đội lốt những thư điện tử, hình ảnh, video trên các mạng xã hội thì dữ liệu của người dùng càng gặp nguy hiểm hơn bội phần nếu lỡ tay nhấn nhầm. Chính vì thế, nếu cảm thấy một nội dung nào đó khả nghi, hãy đóng hoặc xóa chúng ngay lập tức. Cần thường xuyên cập nhật hệ điều hành, trình duyệt web, phần mềm bảo mật. Bởi lẽ các nhà sản xuất phần mềm luôn đặt sự an toàn của người dùng lên hàng đầu và sẽ nhanh chóng tung ra bản cập nhật nếu có một lỗ hổng bảo mật nào đó xuất hiện.

### Sử dụng mật khẩu an toàn trong hệ thống KBNN

Cách đặt và quản lý mật khẩu NSD: Đặt mật khẩu đảm bảo: Độ dài ít nhất là 8 ký tự. Bao gồm cả chữ hoa, chữ thường, số và các ký tự đặc biệt (a-z, A-Z, 0-9, !@#$%^&*()_+=\/{}[]...). Thay đổi mật khẩu theo định kỳ. Không đặt mật khẩu rỗng " " hoặc đặt mật khẩu trùng với tên tài khoản. Không sử dụng các từ dễ đoán để dùng cho mật khẩu (tên người thân, tên cơ quan, biển số xe....). Không sử dụng các chuỗi liên tục (abcde, qwert, 1234...) để làm mật khẩu. Các mật khẩu trên các hệ thống khác nhau của cùng một NSD không đặt trùng nhau. NSD không được chia sẻ mật khẩu của cá nhân với bất kỳ ai, kể cả người quản trị hay người quản lý bộ phận. Tất cả các mật khẩu đều phải được coi là những thông tin nhạy cảm, do đó NSD không được viết lại mật khẩu và lưu trữ nó ở đâu đó trong văn phòng, trong một file nào đó trên máy tính khi chưa được mã hóa. Không chọn chức năng "Ghi nhớ mật khẩu" ở cửa sổ đăng nhập, hoặc chế độ tự động đăng nhập. Khi mất hoặc nghi ngờ lộ mật khẩu hoặc khi được bàn giao mật khẩu mới NSD có trách nhiệm tự đổi mật khẩu ngay lập tức. Khi không có quyền tự đổi mật khẩu, phải thông báo ngay cho bộ phận quản trị để thay đổi mật khẩu mới.

### Truy cập Internet an toàn

Theo Quyết định số 95 /QĐ-KBNN ngày 14/02/2014 của Tổng Giám đốc KBNN về an toàn thông tin đối với người sử dụng hệ thống CNTT trong hệ thống KBNN hướng dẫn sử dụng Internet an toàn cho công chức KBNN, cụ thể: NSD không nên truy cập các trang web lạ không rõ nguồn gốc hoặc các đường dẫn tới các trang web do người lạ gửi tới. NSD cần đọc thật kỹ các yêu cầu xuất hiện trên trang web, nếu thực sự không chắc chắn thì nên đóng các cửa sổ yêu cầu dạng: Cài đặt font chữ mới; cài đặt phần mềm diệt virus lạ; mở tiếp các trang web mới. NSD không nên sử dụng chức năng đăng nhập tự động

*Công chức KBNN vận hành thiết bị tại trung tâm dữ liệu tại KBNN Lào Cai* *Ảnh: NT*

(lưu lại tài khoản và mật khẩu) khi đăng nhập trên môi trường mạng và Internet.

Hiện nay có khá nhiều trang web cung cấp tính năng liên kết với các tài khoản cá nhân người dùng. Điển hình như Google cho phép bạn liên kết nhiều tài khoản Gmail trên cùng một trình duyệt. Ngoài ra, một số trang web khác lại sử dụng cơ chế sử dụng tài khoản Google, Facebook, Apple ID... để đăng nhập tự động.

Tuy mang lại sự tiện lợi nhưng điều này cũng khiến tài khoản của bạn gặp nhiều rủi ro hơn. Nếu một tài khoản bị xâm hại thì tất cả các tài khoản liên kết còn lại đều có thể bị ảnh hưởng tương tự. Vì thế, hãy sử dụng từng tài khoản cá nhân một cách thủ công thay vì tự động như trước kia.

Xóa cache trong tất cả các thiết bị bạn sử dụng trong một ngày như máy tính ở cơ quan, ở nhà, iPad ... Mỗi lần bạn sử dụng trình duyệt như Firefox hay Chrome, nó đều giữ lại thông tin bạn đã truy cập vào đâu và làm gì. Thường thì đây là yếu tố được mặc định, mỗi một trang web mà bạn truy cập và tất cả những gì bạn tải lên mạng hay tải xuống đều lưu lại trên máy trong nhiều ngày hoặc thậm chí nhiều tuần. Chọn Settings/Preferences -> Privacy & Security -> Chọn Cookies and Site Data -> Chọn Clear Data hoặc Check chọn Delete cookies and site data when Firefox/Chrome is closed.

Vì vậy, hãy thường xuyên xóa đi những cache trên trình duyệt của bạn. Việc xoá này vừa đảm bảo an toàn thông tin vừa cải thiện tốc độ truy cập Hệ thống Dịch vụ công của KBNN. Ngoài ra, sau mỗi lần sử dụng web, hãy thoát tài khoản của bạn ra khỏi các trang web, mạng xã hội nhằm tránh những mất mát đáng tiếc có thể xảy ra đặc biệt khi bạn sử dụng máy tính nơi công cộng.

HTTP (một trong những giao thức truyền tải siêu văn bản nền tảng trên Internet, giữa máy tính của người dùng và máy chủ server). HTTPS là một biến thể của giao thức HTTP được thêm vào lớp bảo mật và mã hóa trong khi người sử dụng đang truy cập mạng. Liên lạc giữa người sử dụng và trang web HTTPS được mã hóa và cũng chứng minh sự xác thực, có nghĩa là HTTPS có thể được sử dụng để phát hiện các trang web giả thường được dùng trong kỹ thuật tấn công trung gian "man in the middle". Hiện các ứng dụng web tại KBNN đã sử dụng bảo mật HTTPS.

### Một số hành vi nghiêm cấm khi sử dụng Internet tại KBNN

Chơi trò chơi trên máy tính thuộc hệ thống KBNN, truy cập trang web có nội dung xấu.

Lợi dụng hệ thống mạng Internet để làm rối loạn, cản trở hoạt động cung cấp, sử dụng dịch vụ, truyền bá các thông tin, hình ảnh chống lại Nhà nước, gây rối an ninh trật tự, xâm hại đến lợi ích của các cơ quan, tổ chức, cá nhân; vi phạm đạo đức, thuần phong mỹ tục; xây dựng các trang web, tổ chức các diễn đàn trên Internet có nội dung hướng dẫn, lôi kéo, kích động người khác thực hiện các hành vi trên trái với quy định của pháp luật.

Gửi, lan truyền, phát tán virus tin học, chương trình phần mềm có tính năng lấy trộm thông tin, phá huỷ dữ liệu máy tính lên hệ thống mạng Internet.

Tiết lộ bí mật nhà nước, bí mật quân sự, an ninh, kinh tế, đối ngoại và những bí mật khác đã được pháp luật quy định.

Lợi dụng Internet để quảng cáo, tuyên truyền, mua bán, kinh doanh hàng hoá, dịch vụ thuộc danh mục cấm theo quy định của pháp luật, tổ chức, tham gia các hình thức đánh bạc, cá độ.

Đánh cắp và sử dụng trái phép mật khẩu, khoá mật mã và thông tin riêng của các tổ chức, cá nhân trên Internet.

Nghiêm cấm máy tính dùng để soạn thảo, in ấn, lưu trữ bí mật Nhà nước kết nối Internet.

Không sử dụng máy tính chứa dữ liệu quan trọng hoặc có khả năng tiếp cận các dữ liệu, ứng dụng quan trọng của ngành Tài chính để mở trang tin hoặc ứng dụng Internet trừ trường hợp được phép truy cập: Internet có giới hạn của lãnh đạo đơn vị; NSD tự chịu trách nhiệm cá nhân trước pháp luật về các hành vi, các thông tin do mình đăng tải lên Internet.

*TÀI LIỆU THAM KHẢO:*

*1. Quyết định số 95 /QĐ-KBNN ngày 14/02/2014 của Tổng Giám đốc KBNN về an toàn thông tin đối với người sử dụng hệ thống CNTT trong hệ thống KBNN*

*2. Giáo trình đào tạo An toàn thông tin nâng cao dành cho người dùng Trung ương của Trung tâm đào tạo QNet năm 2019.*

*3.Tạp chí An toàn thông tin: http://antoanthong-tin.vn/ của Ban cơ yếu Chính phủ*

*Ngày nhận bài: 26/02/2021*
*Ngày đưa phản biện: 26/02/2021*
*Ngày chấp nhận đăng: 08/4/2021*
*Email: yennth@vst.gov.vn*