

LUẬT AN NINH MẠNG - NHỮNG ĐIỀU CẦN BIẾT

Luật An ninh mạng là gì? Tìm hiểu nội dung trong luật an ninh mạng

Đến nay vẫn có rất nhiều độc giả chưa biết Luật an ninh là gì, quy định cụ thể như thế nào. Điều này cũng rất dễ hiểu, bộ luật này mới được quy định và chính thức có hiệu lực từ đầu năm 2019 vừa rồi.

Tóm Tắt Nội Dung

- Luật An ninh mạng là gì?
- Phạm vi của luật An ninh mạng
- Luật An ninh mạng trong quy định hệ thống thông tin
- Hành vi bị cấm trên không gian mạng theo luật an ninh mạng
- Luật An ninh mạng giám sát hệ thống thông tin
- Luật an ninh mạng sẽ giám sát nội dung
- Thực thi luật an ninh mạng
- Kết luận

Luật An ninh mạng là gì?

Luật An Ninh mạng là một bộ luật đã được Quốc hội Việt Nam đã thông qua. Luật mới về An ninh mạng có hiệu lực từ ngày 1 tháng 1 năm 2019 tại Việt Nam. Không chỉ cung cấp các biện pháp bảo vệ môi trường mạng mà ở một mức độ nào đó đã được quy định bởi Luật An toàn thông tin mạng ngày 19 tháng 11 năm 2015, Luật An Ninh Mạng cũng bao gồm nhiều điều khoản khác nhau để kiểm soát nội dung được đăng hoặc xuất bản trên mạng. Dưới đây là một số vấn đề nổi bật luật an ninh mạng.

Phạm vi của luật An ninh mạng



Luật An ninh mạng áp dụng cho tất cả các cơ quan, tổ chức, cá nhân liên quan đến bảo vệ an ninh mạng, được định nghĩa rộng rãi là đảm bảo rằng các hoạt động trong không gian mạng

không gây tổn hại đến an ninh quốc gia, trật tự an toàn xã hội, quyền và lợi ích hợp pháp của các cơ quan, tổ chức và cá nhân. Đặc biệt, Luật An ninh mạng sẽ áp dụng cho các tổ chức ở nước ngoài, có người dùng cư trú tại Việt Nam như Google hoặc Facebook.

Luật An ninh mạng bao gồm tất cả các mạng về cơ sở hạ tầng CNTT, viễn thông, Internet, hệ thống máy tính, cơ sở dữ liệu, xử lý thông tin, hệ thống lưu trữ và kiểm soát và điều chỉnh các hoạt động của mọi doanh nghiệp cung cấp dịch vụ trong không gian mạng và người dùng Internet bao gồm thương mại điện tử, trang web, diễn đàn trực tuyến, mạng xã hội và blog.

Luật An ninh mạng áp đặt các nghĩa vụ khác nhau đối với người vận hành hệ thống thông tin. Theo Luật An toàn thông tin mạng theo đó, người vận hành hệ thống thông tin có nghĩa là bất kỳ cơ quan, tổ chức hoặc cá nhân nào có quyền quản lý trực tiếp đối với hệ thống thông tin.

Luật An ninh mạng trong quy định hệ thống thông tin

Luật An ninh mạng phân loại các hệ thống thông tin thành:

- các hệ thống thông tin quan trọng đối với an ninh quốc gia
- các hệ thống không thuộc Hệ thống thông tin quan trọng (Hệ thống thông tin không quan trọng).

Hệ thống thông tin quan trọng: thường được định nghĩa là hệ thống thông tin, nếu gặp sự cố, xâm nhập, chiếm quyền điều khiển hoặc vận hành, bóp méo, gián đoạn, ngừng hoạt động, tê liệt, phá hủy sẽ làm tổn hại nghiêm trọng đến an ninh mạng. Dường như danh sách Hệ thống thông tin quan trọng theo Luật An ninh mạng 2018 rộng hơn so với những gì đã được quy định theo Quyết định 632 của Thủ tướng Chính phủ ngày 10 tháng 5 năm 2017 (Quyết định 632). Hiện tại, Quyết định 632 bao gồm các lĩnh vực viễn thông và mạng lưới thông tin trong các cơ quan của Đảng Cộng sản và chính phủ mà Bộ Thông tin và Truyền thông (MIC) hoặc Văn phòng Chính phủ là quản trị viên (chủ đề). Các hệ thống thông tin quan trọng hiện nay bao gồm hệ thống thông tin trong các lĩnh vực năng lượng, tài chính, ngân hàng, viễn thông, giao thông vận tải, tài nguyên và môi trường, hóa chất, y tế, văn hóa và báo chí. Có lẽ, Quyết định 632 có thể được bổ sung với nhiều lĩnh vực quan trọng đối với an ninh quốc gia và sự tham gia của các bộ liên quan khác ngoài MIC.

Hệ thống thông tin không quan trọng: mặc dù không được xác định rõ ràng, nên là bất kỳ hệ thống thông tin nào được quản lý bởi các tổ chức và doanh nghiệp tư nhân.

Hành vi bị cấm trên không gian mạng theo luật an ninh mạng

LUẬT

AN NINH

MẠNG

QUY ĐỊNH NHỮNG HÀNH VI NÀO BỊ NGHIÊM CẤM?

Luật An ninh mạng 2018 cấm sử dụng không gian mạng để thực hiện bất kỳ hành vi nào sau đây:

- Sử dụng không gian mạng, CNTT và phương tiện điện tử để vi phạm luật pháp về an ninh quốc gia, trật tự và an toàn xã hội;
- Tổ chức, kích hoạt, thông đồng, xúi giục, mua chuộc, lừa đảo hoặc lừa đảo, thao túng, đào tạo hoặc xúi giục, kêu gọi người để chống lại Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam;
- Lịch sử xuyên tạc, phủ nhận thành tựu cách mạng, phá hủy khối đoàn kết dân tộc, tiến hành các hành vi phạm tội chống tôn giáo, phân biệt giới tính hoặc các hành vi phân biệt chủng tộc;
- Cung cấp thông tin sai lệch, gây nhầm lẫn trong công dân, gây tổn hại cho các hoạt động kinh tế xã hội, gây khó khăn cho hoạt động của các cơ quan nhà nước hoặc của người thực hiện công vụ, hoặc xâm phạm quyền và lợi ích hợp pháp của các cơ quan, tổ chức, cá nhân khác;
- Các hoạt động là mại dâm, tệ nạn xã hội hoặc buôn bán người; công bố thông tin là dâm dục, đồi trụy hoặc hình sự; hoặc phá hủy các truyền thống và phong tục tốt đẹp của người dân, đạo đức xã hội hoặc sức khỏe của cộng đồng; và
- Kích động, dụ dỗ hoặc kích hoạt người khác phạm tội.

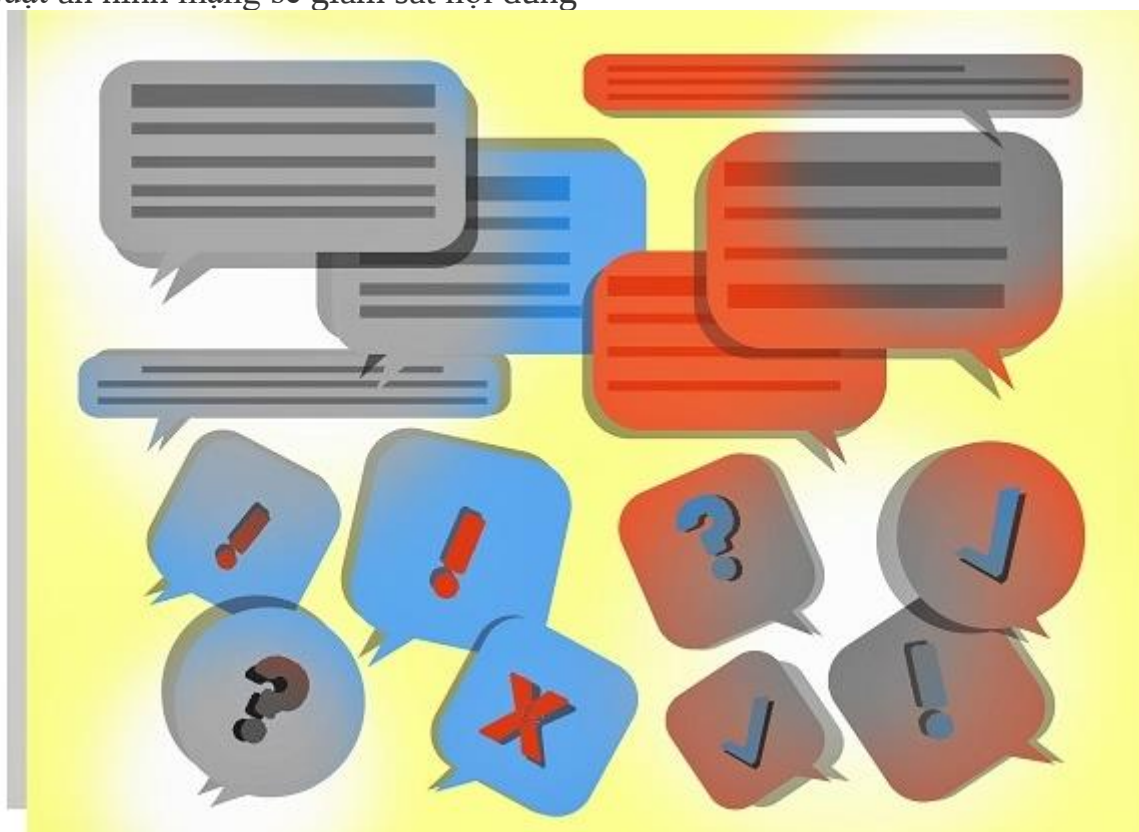
Luận An ninh mạng giám sát hệ thống thông tin

Hệ thống thông tin quan trọng: Hệ thống thông tin quan trọng phải được các cơ quan có thẩm quyền đánh giá và chỉ có thể được đưa vào hoạt động sau khi được chứng nhận là đáp ứng các điều kiện an ninh mạng. Hệ thống thông tin quan trọng có thể được kiểm tra một cách thường xuyên hoặc khi xảy ra một sự kiện được quy định theo luật này. Các nhà điều hành của Hệ thống thông tin quan trọng chịu trách nhiệm giám sát các hệ thống, xây dựng cơ chế cảnh báo tự động và nhận các cảnh báo về các mối đe dọa đối với an ninh mạng và lập kế hoạch đối phó với các tình huống đó.

Hệ thống thông tin không quan trọng: Hệ thống thông tin không quan trọng có thể bị Lực lượng đặc nhiệm an ninh mạng đặt dưới sự kiểm tra an ninh mạng khi vi phạm luật an ninh mạng vi phạm an ninh quốc gia hoặc gây thiệt hại nghiêm trọng cho trật tự và an toàn xã hội. Lực lượng đặc nhiệm an ninh mạng có thể tiến hành kiểm tra sau khi gửi thông báo bằng văn bản ít nhất 12 giờ trước khi kiểm tra cho quản trị viên của Hệ thống thông tin không quan trọng. Các thành phần được kiểm tra bao gồm phần mềm, phần cứng, thiết bị kỹ thuật số; dữ liệu được lưu trữ, xử lý và chuyển giao trong hệ thống; và phương pháp bảo vệ bí mật nhà nước.

Như vậy, Luật An ninh mạng không đặt ra cơ sở và thủ tục rõ ràng để xác định có vi phạm Luật An ninh mạng hay không. Ví dụ, Luật An ninh mạng 2018 cấm sử dụng không gian mạng để bóp méo lịch sử, phủ nhận thành tích cách mạng, phá hủy khối đoàn kết dân tộc, tiến hành phạm tội chống lại tôn giáo, phân biệt giới tính hoặc hành vi phân biệt chủng tộc. Sẽ rất khó và có thể tranh cãi để xác định một hành động là xuyên tạc lịch sử và do đó vi phạm điều khoản đó. Do đó, các quy định có thể tạo ra sự không chắc chắn cho các doanh nghiệp cung cấp dịch vụ trong không gian ảo và giữ dữ liệu của khách hàng trong quá trình cung cấp dịch vụ.

Luật an ninh mạng sẽ giám sát nội dung



Các nhà cung cấp dịch vụ trên không gian mạng tại Việt Nam phải tuân thủ nhiều yêu cầu để giám sát nội dung được tải lên và phổ biến trong không gian ảo:

- Tất cả các trang web, cổng hoặc trang chuyên biệt trên mạng xã hội của các cơ quan, tổ chức và cá nhân không được cung cấp, tải lên hoặc truyền thông tin với tuyên truyền chống lại Nhà nước, kích động bạo loạn, hoặc phá vỡ an ninh hoặc gây rối trật tự công cộng, gây bôi nhọ hoặc gây ra sự xấu hổ hoặc vi phạm lệnh quản lý kinh tế (nội dung bị cấm);

- Để xác minh đăng ký tài khoản của người dùng và cung cấp thông tin của người dùng khi nhận được yêu cầu bằng văn bản từ các cơ quan có thẩm quyền về an ninh mạng;
- Để ngăn chặn việc chia sẻ thông tin và xóa nội dung bị cấm trong vòng 24 giờ sau khi nhận được yêu cầu bởi Luật an ninh sẽ ngay lập tức điều tra và ngừng cung cấp dịch vụ cho các tổ chức và cá nhân tải lên thông tin bị cấm.

Người quản trị mạng có thể rất khó khăn và tốn kém khi xác định và lọc nội dung bị cấm vì một số trong số đó không rõ ràng. Ví dụ, Luật An ninh mạng 2018 xác định thông tin đang tuyên truyền chống lại Nhà nước để bao gồm nội dung:

- (i) xuyên tạc hoặc phỉ báng các cơ quan hành chính nhân dân;
- (ii) khởi xướng chiến tranh tâm lý, kích động chiến tranh xâm lấn, gây chia rẽ hoặc thù hận giữa các nhóm sắc tộc, tôn giáo và người dân của tất cả các quốc gia;
- (iii) xúc phạm người dân, quốc kỳ, quốc huy, quốc ca, đại nhân, lãnh đạo, người nổi tiếng hoặc anh hùng dân tộc.

Khi đọc những hạn chế này, người ta có thể bị nhầm lẫn, ví dụ: Ai được coi là người vĩ đại? Hồi giáo, lãnh đạo, người nổi tiếng hay anh hùng dân tộc?

Liệu một nghiên cứu công khai mới với một quan điểm khác về thành tích của một anh hùng dân tộc Hồi giáo có thể được coi là xúc phạm người anh hùng dân tộc Hồi giáo? quy định này có thể tước quyền của người dân để chỉ trích sự lãnh đạo và quản trị của một hệ thống hành chính hoặc một số quan chức của hệ thống đó?

Thực thi luật an ninh mạng

Các lực lượng chuyên trách chịu trách nhiệm thi hành Luật An ninh mạng (Lực lượng đặc nhiệm an ninh mạng) sẽ được bổ nhiệm thuộc Bộ Công an và Bộ Quốc phòng. Lực lượng đặc nhiệm an ninh mạng có sức mạnh rộng lớn theo Luật An ninh mạng với sự giám sát hạn chế. Ví dụ, Lực lượng đặc nhiệm an ninh mạng không bắt buộc phải tuân theo các quy trình tương tự như các Quy trình tổ tụng hình sự để tiến hành kiểm tra hệ thống thông tin hoặc thu thập dữ liệu người dùng và không bắt buộc phải giữ bí mật thông tin mà họ đang thu thập.

Theo Luật An ninh mạng 2018, hậu quả của việc vi phạm luật về an ninh mạng có thể ở các hình thức kỷ luật, trách nhiệm hành chính hoặc hình sự.

Kết luận

Các yêu cầu của Luật An ninh mạng có thể làm tăng chi phí, trách nhiệm tuân thủ và đặt ra một vấn đề nan giải cho các nhà cung cấp dịch vụ giữa tuân thủ và bảo vệ dữ liệu khách hàng. Nhiều yêu cầu trong Luật An ninh mạng sẽ phải chịu sự hướng dẫn thêm của Chính phủ. Do đó, các tổ chức và cá nhân bị ảnh hưởng nên tiếp tục tuân theo các hướng dẫn luật an ninh mạng để chấp hành tốt nhất.

phapluatvn.vn

MỘT SỐ HÀNH VI VI PHẠM LUẬT AN NINH MẠNG DỄ BỊ MẮC PHẢI

1. Kêu gọi, vận động, xúi giục, đe dọa, lôi kéo tụ tập đông người để gây rối, chống người thi hành công vụ, cản trở hoạt động của cơ quan, tổ chức gây mất ổn định về an ninh, trật tự;
2. Xúc phạm nghiêm trọng danh dự, uy tín, nhân phẩm của người khác;

3. Thông tin bịa đặt, sai sự thật xâm phạm danh dự, uy tín, nhân phẩm hoặc gây thiệt hại đến quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân khác;
4. Thông tin bịa đặt, sai sự thật về sản phẩm, hàng hóa, tiền, trái phiếu, tín phiếu, công trái, séc và các loại giấy tờ có giá trị khác;
5. Thông tin bịa đặt, sai sự thật trong lĩnh vực tài chính, ngân hàng, thương mại điện tử, thanh toán điện tử, kinh doanh tiền tệ, huy động vốn, kinh doanh đa cấp, chứng khoán;
6. Thông tin trên không gian mạng có nội dung bịa đặt, sai sự thật gây hoang mang trong nhân dân, gây thiệt hại cho hoạt động KT-XH, gây khó khăn cho hoạt động của CQNN hoặc người thi hành công vụ, xâm phạm quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân khác;
7. Chiếm đoạt, mua bán, thu giữ, cố ý làm lộ thông tin thuộc bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư gây ảnh hưởng đến danh dự, uy tín, nhân phẩm, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân;
8. Đưa lên không gian mạng những thông tin thuộc bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư trái quy định của pháp luật;
9. Cố ý nghe, ghi âm, ghi hình trái phép các cuộc đàm thoại;
10. Đăng tải phát tán thông tin trên không gian mạng có nội dung quy định tại các khoản 1, 2, 3, 4 và 5 Điều 16 và hành vi quy định tại khoản 1 Điều 17 của Luật An ninh mạng;
11. Chiếm đoạt tài sản; tổ chức đánh bạc, đánh bạc qua mạng Internet; trộm cắp cước viễn thông quốc tế trên nền Internet; vi phạm bản quyền và sở hữu trí tuệ trên không gian mạng;
12. Tuyên truyền, quảng cáo, mua bán hàng hóa, dịch vụ thuộc danh mục cấm theo quy định của pháp luật;
13. Hướng dẫn người khác thực hiện hành vi vi phạm pháp luật;
14. Phát tán chương trình tin học gây hại cho mạng viễn thông, mạng Internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu, phương tiện điện tử.



16 THỦ ĐOẠN LỪA ĐẢO TRÊN KHÔNG GIAN MẠNG



1. GIẢ DANH CÔNG AN, VIỆN KIỂM SÁT

Giả danh là cán bộ Công an, Viện kiểm sát thông báo vi phạm, yêu cầu nạn nhân phải chuyển tiền/cài đặt ứng dụng "Bộ Công an" rồi chiếm đoạt.



2. LỪA TÌNH, LỪA TIỀN TỬ THIỆN

Giả làm quân nhân, doanh nhân, người nước ngoài muốn gửi quà có giá trị hoặc tiền từ thiện về Việt Nam. Sau đó, giả làm hải quan yêu cầu đóng phí cho chúng rồi chiếm đoạt.



3. LỪA ĐẢO MUA BÁN HÀNG TRỰC TUYẾN

Gửi đường dẫn thanh toán giả mạo để chiếm đoạt tiền trong tài khoản ngân hàng. Yêu cầu chuyển cọc trước sau đó chiếm đoạt tiền cọc.



4. GIẢ NHÂN VIÊN NGÂN HÀNG HỖ TRỢ KỸ THUẬT

Giả danh là nhân viên ngân hàng hướng dẫn kiểm tra tài khoản hoặc nâng cấp ứng dụng để chiếm đoạt tiền trong tài khoản ngân hàng.



5. LỪA ĐẢO QUA HÌNH THỨC TRÚNG THƯỞNG

Giả danh là nhân viên công ty, ngân hàng gọi điện thông báo trúng thưởng (tiền, quà có giá trị), yêu cầu đóng phí để nhận thưởng rồi chiếm đoạt.



6. HACK FACEBOOK, ZALO LỪA ĐẢO MƯỢN TIỀN

Chiếm quyền tài khoản Facebook, Zalo sau đó nhắn tin hỏi mượn tiền bạn bè. Số tài khoản nhận tiền luôn là số tài khoản không chính chủ.



7. LỪA ĐẢO TÌM NGƯỜI LÀM VIỆC TẠI NHÀ

Công việc: lắp ráp bút bi, dán tem son, khâu vòng, ... Muốn nhận sản phẩm về nạn nhân phải đặt cọc. Sau khi nhận cọc xong của nạn nhân thì chiếm đoạt.



8. MẠO DANH CÔNG TY TÀI CHÍNH LỪA VAY

Chủ động liên hệ nạn nhân hứa hẹn cung cấp những khoản vay lãi suất thấp, thủ tục đơn giản. Yêu cầu đóng phí vay, phí để sửa thông tin trong hồ sơ rồi chiếm đoạt.



- **KHÔNG** chuyển tiền cho bất kỳ ai mà chưa biết rõ về họ.
- Cơ quan nhà nước **KHÔNG** làm việc qua ĐIỆN THOẠI, nếu cần sẽ mời qua trụ sở.
- Khi người thân, người quen hỏi mượn tiền, nhờ chuyển tiền. **HÃY GỌI ĐIỆN THOẠI** số chính chủ để xác nhận lại.
- Tuyệt đối **KHÔNG CUNG CẤP** số OTP, tài khoản E-Banking cho bất kỳ ai.
- Đa số các cách kiếm tiền dễ dàng trên MXH đều là "quả lừa", "bánh vẽ". **HÃY CẢNH GIÁC!**



16 THỦ ĐOẠN LỪA ĐẢO TRÊN KHÔNG GIAN MẠNG



9. MẠO DANH CÔNG TY BẢO HIỂM XÃ HỘI

Thông báo bạn nợ tiền hoặc trục lợi quỹ Bảo hiểm xã hội. Yêu cầu đóng phí, nếu không họ sẽ báo Công an.



10. CỐ TÌNH CHUYỂN KHOẢN NHẪM ĐỂ ÉP VAY

Giả chuyển khoản nhầm và yêu cầu nạn nhân chuyển lại vào tài khoản khác. Sau một thời gian, quay lại đòi đóng lãi nếu không sẽ kiện ra tòa và quấy rối.



11. LỪA NÂNG CẤP SIM 4G

Giả nhân viên nhà mạng đề nghị nâng cấp Sim. Sau khi nạn nhân nhấn tin theo cú pháp được hướng dẫn sẽ mất quyền kiểm soát sim dẫn đến mất các tài khoản ngân hàng, mạng xã hội liên kết với sim của nạn nhân.



12. LẬP SÀN GIAO DỊCH TIỀN ẢO, CHỨNG KHOÁN

Quảng cáo hấp dẫn về lời nhuận để thu hút người chơi, khi người chơi nạp số tiền lớn vào sàn hoặc vào ứng dụng thì không cho rút tiền.



13. LỪA ĐẢO "CHO SỐ LÔ, SỐ ĐẾ"

Để nhận được số người chơi phải đóng phí, nếu không trúng thì mất phí. Nếu trúng thì phải chia hoa hồng cho các đối tượng. giá trị), yêu cầu đóng phí để nhận thưởng rồi chiếm đoạt.



14. LÀM NHIỆM VỤ QUA ỨNG DỤNG, TUYỂN CỘNG TÁC VIÊN

Làm nhiệm vụ: thanh toán đơn hàng Shopee, Tiki, theo dõi Facebook, Tiktok người nổi tiếng,... Từ 1 đến 2 lần đầu sẽ được hoàn tiền, khi nhiệm vụ có số tiền lớn hơn sẽ bị lỗi, đóng liên tiếp/ không đóng đều mất tiền.



15. GIẢ DANH CÁN BỘ VIÊN THÔNG, CỤC VĂN THƯ

Thông báo nạn nhân nợ cước hoặc tín dụng sau đó chuyển sang bên xưng là Công an để yêu cầu nạn nhân đóng tiền cho chúng để phục vụ "điều tra".



16. GIẢ MẠO LÃNH ĐẠO TỈNH, SỞ, BAN NGÀNH

Lập tài khoản mạng xã hội (Facebook, Zalo, ...) sử dụng hình ảnh, uy tín lãnh đạo nhân tín cấp dưới để mượn tiền. đơn giản. Yêu cầu đóng phí vay, phí để sửa thông tin trong hồ sơ rồi chiếm đoạt.

**KHUYẾN
CẢO**

- **KHÔNG** chuyển tiền cho bất kỳ ai mà chưa biết rõ về họ.
- Cơ quan nhà nước **KHÔNG** làm việc qua ĐIỆN THOẠI, nếu cần sẽ mời qua trụ sở.
- Khi người thân, người quen hỏi mượn tiền, nhờ chuyển tiền. **HÃY GỌI ĐIỆN THOẠI** số chính chủ để xác nhận lại.
- Tuyệt đối **KHÔNG CUNG CẤP** số OTP, tài khoản E-Banking cho bất kỳ ai.
- Đa số các cách kiếm tiền dễ dàng trên MXH đều là "quả lừa", "bánh vẽ". **HÃY CẢNH GIÁC!**