

Nâng cao nhận thức về tầm quan trọng của an toàn thông tin là bảo vệ chính bạn và doanh nghiệp của bạn!

- ❖ Làm thế nào để tăng nhận thức của nhân viên về tầm quan trọng của thông tin mà doanh nghiệp phải bảo vệ, ví dụ thông tin cá nhân và thông tin bán hàng, v.v, cũng như ý thức được mức độ nguy hại khi thông tin của doanh nghiệp bị rò rỉ?
- ❖ Làm thế nào để nhân viên đề cao cảnh giác và biết cách phòng tránh, đối phó trước các sự cố rò rỉ thông tin do tấn công mạng hay gian lận email doanh nghiệp, trong khi các thủ đoạn lấy cắp thông tin ngày càng tinh vi và khó lường hơn?
- ❖ Làm thế nào để xây dựng và vận hành nội quy bảo mật thông tin của toàn công ty, qua đó có 1 quy chế rõ ràng để nhân viên tuân thủ an toàn thông tin trong doanh nghiệp?

⇒ Khóa học “**Nâng cao nhận thức an toàn thông tin**” và chương trình tư vấn “**Hỗ trợ thiết lập Nội quy bảo mật thông tin**” sẽ giúp học viên và doanh nghiệp nâng cao nhận thức, trang bị các kiến thức, kỹ năng và giải pháp cụ thể để có thể truy cập Internet, sử dụng E-Mail, mạng xã hội và mạng nội bộ công ty một cách an toàn và bảo mật.

NÂNG CAO NHẬN THỨC AN TOÀN THÔNG TIN

Đối tượng: Nhân viên Việt Nam, nhân viên đào tạo nội bộ về an toàn thông tin.

Mục tiêu

- Hiểu rõ các khái niệm an toàn thông tin như bảo mật, lỗ hổng, tấn công mạng.
- Nhận biết các nguy cơ có thể bị lợi dụng để trục lợi qua đó có thể tự bảo vệ mình và chủ động phòng tránh cho bản thân và doanh nghiệp.
- Nâng cao nhận thức bảo vệ máy tính và dữ liệu, thông tin cá nhân và của doanh nghiệp trước các nguy cơ rò rỉ thông tin khi sử dụng internet, các thiết bị lưu trữ ngoài.

NỘI DUNG ĐÀO TẠO (1 ngày)

Phần 1: An toàn thông tin là gì?

1. Khái niệm về an toàn thông tin.
2. Các loại thông tin cá nhân và trong doanh nghiệp cần bảo mật.
3. Vì sao cần đảm bảo an toàn thông tin cho cá nhân và doanh nghiệp?

Phần 2: An toàn khi sử dụng máy tính và các thiết bị di động

1. Các điều cơ bản khi sử dụng máy tính: ID, Password, phần mềm có bản quyền.
2. Kiến thức cơ bản về virus máy tính, phần mềm độc hại, phần mềm gián điệp, lỗ hổng phần mềm...
3. Những điều cần làm khi rời khỏi máy tính, sử dụng máy tính cá nhân ngoài nơi làm việc.
4. An toàn khi sử dụng các thiết bị di động.

Phần 3: An toàn khi sử dụng E-mail và mạng Internet

1. Lưu ý để gửi và nhận E-mail an toàn.
2. Nhận biết và phòng tránh E-mail lừa đảo (Phishing).
3. Vấn đề khi “lướt web” và thực hiện các giao dịch trực tuyến.
4. Những chú ý khi sử dụng mạng xã hội.
5. Mỗi nguy hiểm khi sử dụng mạng không dây.
6. Các vấn đề cần lưu ý khi làm việc từ xa.
7. Phòng tránh các cuộc tấn công dựa vào việc lừa đảo (Social engineering).

Phần 4: Nguy cơ rò rỉ thông tin trong doanh nghiệp và đối sách ngăn ngừa

1. Các nguy cơ rò rỉ thông tin mà doanh nghiệp hay gặp phải và cách phòng tránh.
2. Các biện pháp xử lý khi xảy ra sự cố rò rỉ an toàn thông tin.

Phần 5: Tóm tắt và Kế hoạch áp dụng

Hỗ trợ thiết lập “Nội quy bảo mật thông tin”

Mục tiêu:

Giúp Quý công ty thiết lập các qui định liên quan đến các quy tắc để tăng tính bảo mật cho thông tin, tài liệu của Công ty.



Các bước thực hiện chính:

Aimnext đề xuất nội dung các qui định khách hàng muốn thực hiện.

Khách hàng xem xét và phản hồi nội dung.

Aimnext chỉnh sửa Nội quy.

Hoàn thành bản Nội quy.

Nội dung cụ thể sẽ thay đổi tùy theo nội dung thảo luận với khách hàng.

Ví dụ: “Nội quy bảo mật thông tin”

1. Định nghĩa chung
 - Bảo mật thông tin là gì
 - Trách nhiệm của công ty
 - Trách nhiệm của nhân viên
2. Quy tắc về sử dụng tài liệu
 - Quy tắc quản lý tài liệu
 - Quy tắc quản lý tài liệu điện tử
3. Quy tắc sử dụng và bảo quản máy tính
4. Quy tắc sử dụng phần mềm
5. Quy tắc sử dụng email
6. Quy tắc về mật mã
7. Quy tắc sử dụng thiết bị di động