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 tầm quan trọng của thông tin cá nhân, thông tin của doanh nghiệp và an toàn thông tin.
- Nhận biết các mối đe doạ an toàn thông tin của cá nhân và doanh nghiệp, qua đó có thể tự bảo vệ mình và chủ động phòng tránh cho bản thân và doanh nghiệp.
- Nắm được nguyên tắc và các bước cơ bản khi xử lý sự cố rò rỉ thông tin.

NỘI DUNG ĐÀO TẠO (1 ngày)

Phần 1: An toàn thông tin là gì?

1. Thông tin cá nhân và thông tin của doanh nghiệp là gì?
2. Tầm quan trọng của thông tin trong doanh nghiệp
3. An toàn thông tin là gì?

Phần 2: Các mối đe dọa an toàn thông tin trong doanh nghiệp

1. Phần mềm độc hại: virus máy tính, phần mềm độc hại, phần mềm gián điệp…
2. Lừa đảo "câu thông tin" - Phishing
3. Tấn công zero-day
4. Các cuộc tấn công phi kỹ thuật - Social engineering
5. Lỗi do con người

Phần 3: Đối sách an toàn thông tin

1. Sử dụng máy tính
2. Sử dụng các thiết bị di động
3. Sử dụng email
4. Sử dụng mạng và thực hiện các giao dịch trực tuyến
5. Sử dụng Wifi nơi công cộng
6. Sử dụng mạng xã hội
7. Lưu ý khi làm việc từ xa.

Phần 4: Xử lý sự cố rò rỉ thông tin

1. Nguyên tắc khi xử lý sự cố
2. Các bước thực hiện

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

AIMNEXT VIETNAM CO., LTD.
Nam Giao Building 1, 261 – 263 Phan Xich Long,
Ward 2, Phu Nhuan District, Ho Chi Minh City
TEL : (028) 3995 8290
FAX : (028) 3995 8289
Email : training-vn@aimnext.com
URL : www.aimnext.com.vn