SANS SECURITY AWARENESS

安全意识部署指南-
安全在家办公

执行摘要

受冠状病毒影响，许多组织都需要让职工转为在家办公。这可能是一项挑战，因为许多组织缺乏政策、技术和培训以保障远程工作安全。此外，许多职工不熟悉或不习惯在家办公的概念。此指南的目的是使你快**速培**训这一类人，尽量保障其安全。如果你对于如何使用此指南有任何疑问，请通过support@sans.org**与我**们联系。

由于你的职工很可能正在经历巨大的压力和变动，而你的组织很可能时间和资源有限，此战略指南将尽可**能**简化培训。我们建议你仅关注最重要且影响最大的风险，我们会在下文中描述。作为出发点思考这些内**容。如果你**还想要补充额外风险或话题，请务必添加。要意识到，你要求职工遵守越多行为、程序或技，**他**们就越不可能全部执行。

如何使用此指南

我们建议你首先阅读此指南中的材料，并查看不同材料的链接，从而了解可获得的内容。你会注意到，对**于每一个**风险，我们都提供了多个不同材料供你用来吸引和培训你的组织。这使你能够选择满足自己需求**和文化的最有效的形式。当你**阅读完此文件后，请阅读工具包中配备的沟通模板和情况说明，以更好地了**解你**试图达成的目标。一旦你阅读过文件，那么你就需要协调两个关键群体。

1. **安全团队**：协调你的安全团队，更好地了解你试图应对的关键风险是什么。我们已经在此指南中提出**了我**们认为职工在家办公的最大风险，但是你的风险可能不同。警告，安全团队常犯的错误就是试图应对所有风险，使人们被大量政策和要求压垮。尽量试图将需要解决的风险降至最少。一旦你找到这些风险，并为解决这些风险的轻重缓急排序后，请确认可以应对这些风险的行为。正如上文中提到的，如果**你的**组织在这方面没有时间或资源，那么就利用我们记录在以下的内容。

2. **沟通**：**当你找到最大的人力**风险以及应对这些风险的关键行为后，与你的通讯团队合作，让你的雇员**参与并**执行这些行为。最有效的安全意识项目与通讯团队的合作息息相关。如果可行的话，你甚至可以**将通**讯团队的某个成员派遣至安全团队。当与雇员沟通时，可用来鼓励他们参与的有效方式之一是强调**培**训不仅能够保障他们的工作安全，还能保护他们自己和家人，为他们创造安全的家用网络。

最终，通过与这两个群组共同运作，你不仅可以让安全变得简单，还能激发雇员的积极性，[这是行为改变的两个关键元素。]

我们建议你甚至创建一个由关键人员组成的咨询委员会，根据其反馈和投入的信息实施项目。除了安全和**通**讯团队，其他你可能需要合作和协调的部门包括人力资源和法务部门。

MGT433 数字下载包

SANS Institute**提供了**为期两天的培训科目MGT433：如何打造、维系和评估高效的安全意识项目。这一紧凑的课程将提供建立高效安全意识项目的所有理论、技能、框架和资源，使你能够有效应对和衡量你的**人力**风险。在此指南中，我们提供了课程的模板和规划资源数字下载包，可免费使用。这些材料很可能不仅能满足本方案的需求，还能在更大的组织机构或更复杂的部署方案中发挥作用。

回复雇员的问题

除了与职工沟通并对其进行培训，我们还强烈建议使用某些类型的技术或论坛，让你能够回答人们的问题，最好是实时的。这包括专用的邮箱别名、Skype **或** Slack **聊天**频道，或者 Yammer **等在**线论坛。**另一个思路就是**举办安全网络广播，你可以一周重复几次，这样人们就能选择最合适的时间参与事件的直**播**，**甚至可以提出**问题。这样做的目标是你希望尽量将安全变得易于理解，并帮助存有疑问的人。这是吸**引**职工参与安全学习，使这一过程变得友好的绝妙机会，请尽量善加利用这一方式。记住，为了有效实施，你需要分配专员使用任意安全渠道并积极回答问题。

风险与培训材料

我们已经找出了你需要为远程职工处理的三个核心风险。这些不仅是出发点，也很可能是会对你有最大价值的方面。下面每一个风险都关联了多个资源，有助于对话题进行沟通和培训。我们提供多个沟通材料，你可以选择对你的企业文化最有效的材料。此外，几乎所有材料都配备了多语种版本。如果这些材料过多，而你的时间极其有限，那么我们建议你只使用并部署以下两个材料内容。

1. **安全在家**办公情况说明（含在你的部署工具包中）
2. 创造安全的家用网络视频（英语）这里同样也支持其他语言

社会工程学

对远程职工而言，尤其是在这次变化巨大和紧迫的环境下，面临的最大风险之一就是社会工程学。社会工程学是一种心理攻击，攻击者欺骗或诱使他们的目标犯错，在巨变和困惑期则更加容易。关键在于，培训人们社会工程学是什么、如何识别最常见的社会工程学攻击迹象，以及识别出来后该怎样做。确保你不仅重视网络钓鱼攻击，还有其他形式，包括电话、短信、社交媒体或虚假新闻。你可以在我们的社会工程学支持材料文件夹里找到所需要的材料，来对这一话题进行培训和补充。此外，这里还有两个你可以链接的 SANS 安全意识视频，而且也提供了多语言版本。

- 社会工程学（英语）这里同样也支持其他语言
- 网络钓鱼（英语）这里同样也支持其他语言

强密码

正如 Verizon 在其年度数据泄露调查报告中指出的，弱密码是全球范围入侵的主要驱动之一。以下列出了四个关键行为，能够帮助应对这一风险。需要进行培训和强化这一话题以及四个关键行为的材料，可以在密码 文件夹中找到。

- 密文（注意，密码的复杂性和密码有效期已失效）。
- 为所有账号设置独一无二的密码
- 密码管理器
- MFA（多因素验证）通常被称为双因素验证或两步验证

系统更新

第三个风险是确保雇员使用的任何技术都运行最新版本的操作系统、程序和手机应用。人们使用个人设备时，可能需要开启自动更新功能。需要进行培训和强化这一话题的材料，可以在恶意软件或创造安全的家用网络文件夹中里找到。

额外需要考虑的话题

- **Wi-Fi**：保障你的Wi-Fi接入点安全。
  这个话题在创造安全的家用网络材料中有所涉及。另外，请考虑观看视频创造安全的家用网络视频（英语）同样支持其他语言。

- **VPN**：什么是 VPN以及你为什么要使用 VPN。我们推荐关于 VPN 的OUCH 新闻简报。

- **远程工作**：这是为了远程工作的人员，比如咖啡厅、机场航站楼或酒店，并非在家办公的人员。考虑使用我们的远程工作培训视频（英语）同样支持其他语言。

- **孩子/客人**：为了强调家人/客人不可使用工作相关设备，请考虑使用远程工作培训视频（英语）同样支持其他语言。

- **侦测/响应**：如果人们认为在家办公时发生了入侵事件，你是否希望他们上报？如果是，那么你希望他们何时报告和报告什么内容？这包含在我们的遭遇入侵材料中。

OUCH 新闻简报

此外，考虑使用公开的 OUCH 新闻简报支持你的项目，每个都被翻译成了20多种语言。以下列举的是我们认为对你的安全在家办公方案最有用的 OUCH 新闻简报。你可以在线上 OUCH 安全意识新闻简报档案中找到所有简报.

综述

Four Steps to Staying Secure（保障安全的四个步骤）
https://www.sans.org/security-awareness-training/resources/four-simple-steps-staying-secure

Creating a Cybersecure Home（创造安全的家用网络）
https://www.sans.org/security-awareness-training/ouch-newsletter/2018/creating-cybersecure-home

社会工程学

Social Engineering（社会工程学）
https://www.sans.org/security-awareness-training/ouch-newsletter/2017/social-engineering

Messaging / Smishing（消息/短信诈骗）
https://www.sans.org/security-awareness-training/resources/messaging-smishing-attacks

Personalized Scams（个性化诈骗）
https://www.sans.org/security-awareness-training/resources/personalized-scams

CEO Fraud（首席执行官诈骗）
https://www.sans.org/security-awareness-training/resources/ceo-fraudbec

Phone Call Attacks / Scams（电话攻击/诈骗）
https://www.sans.org/security-awareness-training/resources/phone-call-attacks-scams

Stop That Phish（停止网络钓鱼）
https://www.sans.org/security-awareness-training/resources/stop-phish

Scamming You Through Social Media（社交媒体诈骗）
https://www.sans.org/security-awareness-training/resources/scamming-you-through-social-media

密码

Making Passwords Simple（让密码简单化）
https://www.sans.org/security-awareness-training/resources/making-passwords-simple

Lock Down Your Login (2FA)（锁定你的登录（2FA））
https://www.sans.org/security-awareness-training/ouch-newsletter/2017/lock-down-your-login

额外内容
Yes, You Are a Target（没错，你就是目标）
https://www.sans.org/security-awareness-training/resources/yes-you-are-target

Smart Home Devices（智能家用设备）
https://www.sans.org/security-awareness-training/resources/smart-home-devices

小提示

可轻松分享格式的提示和技巧。

- 保障家用无线网络安全最有效的措施就是更改默认管理员密码、开启 WPA2 加密并为你的无线网络设置强密码。
- 要了解所有连入你家用网络的设备，包括婴儿监视器、游戏机、电视、其他家用电器，甚至是你的汽车。确保使用强密码保护所有设备，并且/或者其运行最新版本的操作系统。
- 保护家用电脑最有效的方式之一就是确保操作系统和应用程序都安装了补丁并且更新至最新。如有可能，开启自动更新功能。
- 最后，常识是你的最佳保护。如果邮件、电话或者在线消息看起来奇怪、可疑或是好到令人难以置信，那么这可能就是攻击。
- 确保你的每个账户都使用了独立且唯一的密码。记不住所有的密码/密文？考虑使用密码管理器安全存储所有密码。
- 两步验证是你可以用来保护任何账户安全最好的措施之一。两步验证需要你使用密码的同时，还需要使用发送至你的移动设备或由其生成的验证码。支持两步验证的服务包括 Gmail、Dropbox 和 Twitter。
- 网络钓鱼就是攻击者试图欺骗你点击恶意链接或打开邮件中的附件。怀疑任何营造紧迫感、拼写错误或称呼你为"亲爱的顾客"的邮件或在线消息。

指标

在这种情况下的行为指标较为困难，因为人们在家中的行为更难评估。此外，有些行为并非工作专属（例

如保护他们的Wi-Fi设备）。

然而，你可以评估雇员的参与度。我们发现，这类个人或情感话题非常吸引人，人们对此的兴趣比对其他话题的兴趣更大。因此，这样的指标可能很有价值。

- **互动**：人们在你主持的任何安全渠道或论坛提出问题、发表看法或寻求帮助的频率是怎样的？
- **模拟**：进行某类社会工程学模拟，比如网络钓鱼、短信或电话攻击。

如需更加全面的指标清单，请从 MGT433 数字下载包中下载交互式安全意识指标表格。

许可证

版权所有 © 2020年，SANS Institute。SANS Institute版权所有。未经SANS Institute书面许可，用户不得基于文档的所有或任意部分，在任何印刷、电子或其他媒介中，以任何目的复制、印制、再版、散播、展示、修改或创建衍生产品。此外，未经SANS Institute书面许可，用户不得以任何方式、形态或形式销售、租赁、交易或以其他方式转让这些文档。

部署工具包作者

兰斯·施皮茨纳在网络威胁研究、安全架构、安全意识及安全培训方面有20多年的经验。他创造了蜜网并成立蜜网项目，帮助开辟了诈骗和网络情报领域。作为 SANS 的讲师，他开发了MGT433：安全意识和MGT521：安全文化课程。此外，兰斯还发表了三本关于安全的书籍，为超过25个国家提供过咨询，并帮助超过350个组织结构建立安全意识和安全文化项目，以帮助他们应对人力风险。兰斯是一个积极分享的人，他的推特一直在更新（@lspitzner），并且从事大量群体安全项目。在从事信息安全工作之前，施皮茨纳先生是军队的快速部署部队的防御军官，并且获得了伊利诺伊大学工商管理学硕士学位。

关于SANS Institute

SANS Institute成立于1989年，是一个合作研究和教育机构。SANS 为全球政府和商业机构专业人员提供网络安全培训和认证，是最可靠也是目前最大的此种服务提供商。知名的 SANS 讲师教授60多种不同的课程，进行200多场线下和线上网络安全培训。GIAC 是SANS Institute的分支机构，可为从业者提供超过35种实用的技术性网络安全证书资质认证。SANS Technology Institute 是通过地方资质认证的独立子公司，提供网络安全硕士学位。SANS 为信息安全群体提供大量免费资源，包括已达成共识的项目、研究报告和新闻简报。同时，SANS 还运营着互联网预警系统，即互联网风暴中心。SANS 内部有许多安全领域从业人员，他们代表了从公司到大学等全球的各个组织机构，携手合作，帮助整个信息安全群体。（https://www.sans.org）