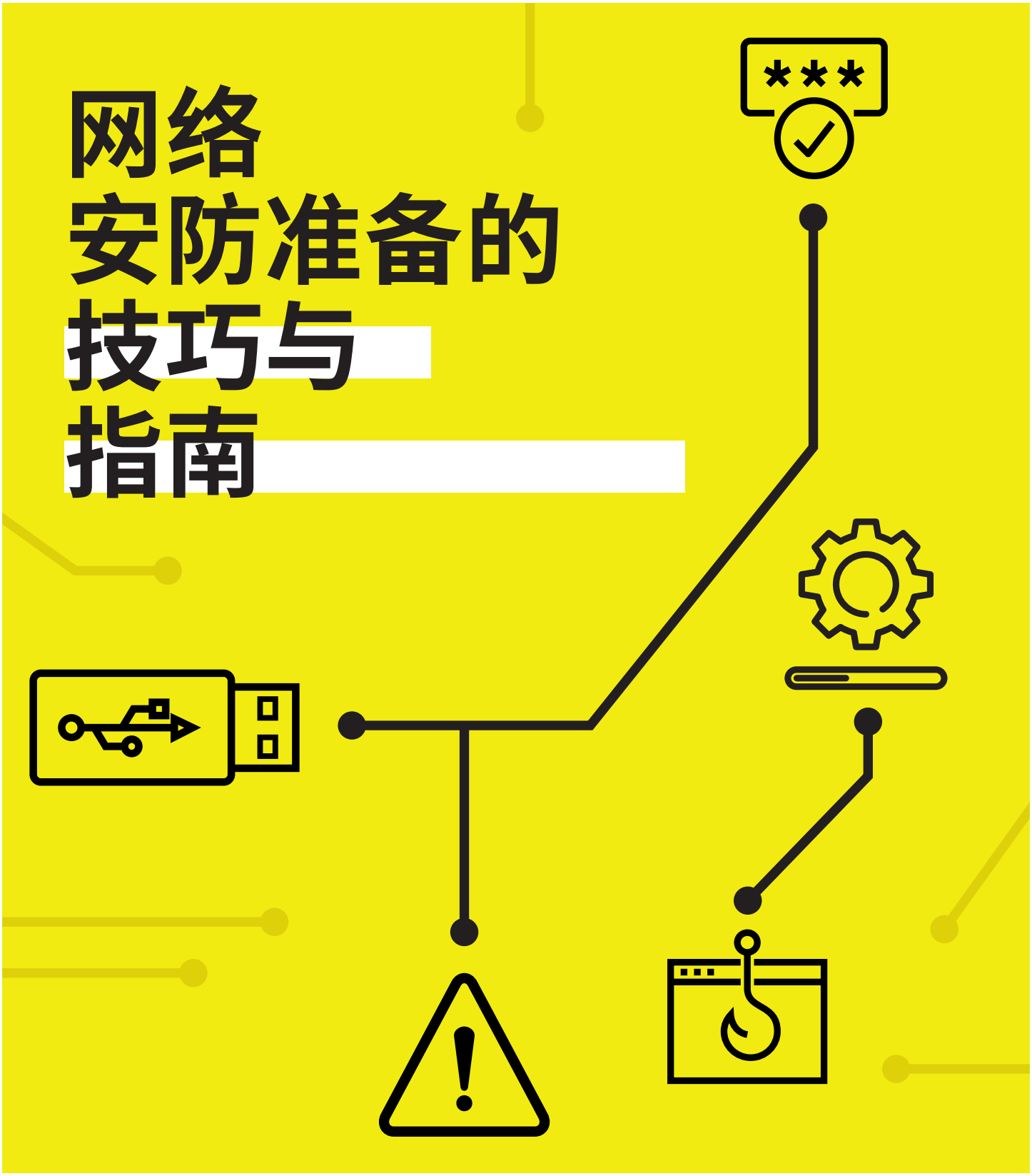
网络安防准备
研究所

网络安防准备的技巧与指南



技巧与
指南

网络安防准备
研究所

大多数公司都要求员工遵守基本的职责，比如准时上班、上班时的着装、如何申请休假等，那么网络安防准备相关的指导方针也应该包括在内。 毕竟您的数据和系统的安全性对您的和业务和客户有很大的影响。 我们建议您使用以下技巧和指导方针来帮助通知您的员工，从而让所有团队成员明白自身责任 并创建一种网络安防准备就绪的氛围。

密码

强度高的密码对保护您的系统和账户至关重要。
无论您是访问工作邮件、从共享硬盘中检索文件还是登陆到任何在线服务，您使用的密码或密码短语都很重要。您甚至可以使用双重身份验证添加另一层安全性。双因素要求您输入唯一的代码，每次新设备登陆要求将代码发送到您的移动设备。双因素身份验证在密码和人之间创建了一个重要的安全链接。

我们鼓励您为员工使用以下指南：

1. 使用包括特殊字符的长密码，例如从您最喜欢的电视节目、电影或歌曲中挑选一句台词。

2. 个人和工作账户永远不要使用相同密码。不要与任何人分享您的用户名和密码，即使是团队成员。

3. 在所有条件允许的情况下使用双因素验证。

软件更新

保持软件和操作系统的更新是非常重要的。
软件供应商发布的每个更新都可能包括重要的补丁，以保护您的软件和系统免受攻击。许多公司指派一个人来管理公司所有计算机的更新，这是较好的办法。或者，您可以要求每个员工管理他们的更新。不论如何，定期更新都是至关重要的。

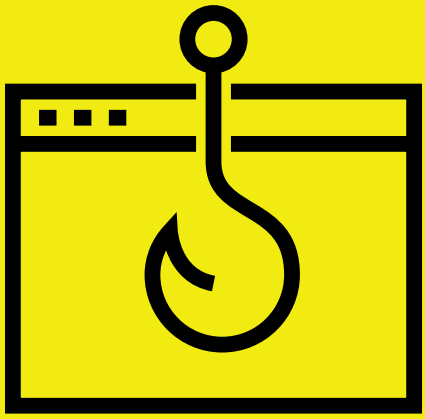
我们建议一下更新指引：

1. 打开所有设备和软件的自动更新功能。

2. 一旦受到更新通知，就会定期更新所有电脑、手机和平板电脑的操作系统、软件和应用程序。

3. 更新所有软件和应用程序，包括公司发布的软件和员工下载的软件。

补丁



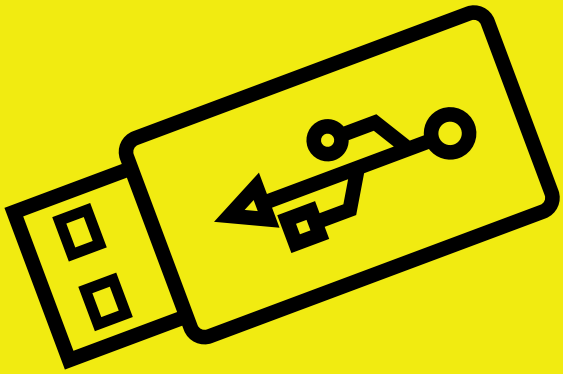
网络钓鱼是目前最常见、最危险的网络问题之一。
一封钓鱼邮件通常看起来像一个真实安全的信息，但打开它可能会导致下载软件病毒或让攻击者访问您的数据。每个人都会收到钓鱼邮件，这就是为什么知道要注意什么是很重要。防范网络钓鱼最好的方法就是提高警惕。

以下是一些有用的建议：

1. 检查发件人的电子邮件和其它识别信息，如公司标识、街道地址和联系方式，从而发现不一致或伪造的信息。

2. 对于不熟悉的发件人，请不要单击任何链接或下载电子邮件中的任何附件。

3. 删除所有可疑邮件并及时清空您的垃圾箱。



USB和可移动媒介

可以在计算机之间方便地共享文件，但它们也可以用来传递病毒和恶意软件。 没有办法知道是谁损坏了驱动，避免USB驱动和其它可移动媒介传播风险的最佳方法是完全避免使用它们。然而，完全禁止USB可能是一个挑战。

因此，我们建议所有员工遵循以下指导方针：

1. 为USB驱动引入易于使用的替代品，例如基于云的文件共享服务，这样USB就没那么必要使用了。

2. 设置一台没有连接到公司网络的计算机，它可以被用作扫描USB中是否有恶意软件，并从USB设备删除需要的信息。

3. 最重要的是，要有良好的判断力，不要插入不知来源的USB驱动。

事件响应

网络安防准备是指采取正确的步骤来降低风险，同时也包括在发生意外时做好准备。制定事件响应计划是做好网络安防准备关键的一步。把它想象成一次消防演习—如果真的发生紧急情况，制定一个让每个人都知道自己角色的计划是很重要的。

你会在网络安防准备项目中找到更多关于事件响应的信息，但至少要关注以下三个方面：

1. 准备。确保所有员工定期备份他们的工作和数据。

2. 响应。如果发生攻击或发现问题，立即将受影响的设备从公司网络断开。所有的员工都必须做这一步。

3. 恢复。从备份中恢复丢失的数据，并将该事件作为一个学习经验以加强网络安防准备原则的重要性，例如密码安全、软件更新、钓鱼意识和USB安全。

准备好把你的技能
提升到下一个水平了吗?

探索
网络安防准备计划

网络安防准备计划是一个免费的在线资源。它列出了您可以采取的实际步骤来评估和提升您的网络安防准备水平。

它易于使用，易于跟踪您的进度，您可以按照自己的节奏来工作。

完成后，您将收到网络安防就绪证书，向客户和供应商表明您已采取步骤在整个企业内创建网络安防准备文化。

了解更多:

https://cyberreadinessinstitute.org/zh/the-cyber-readiness-program