AsiaInfo | 亚信安全

远程办公期间的数据安全防护

远程办公主要形式和问题

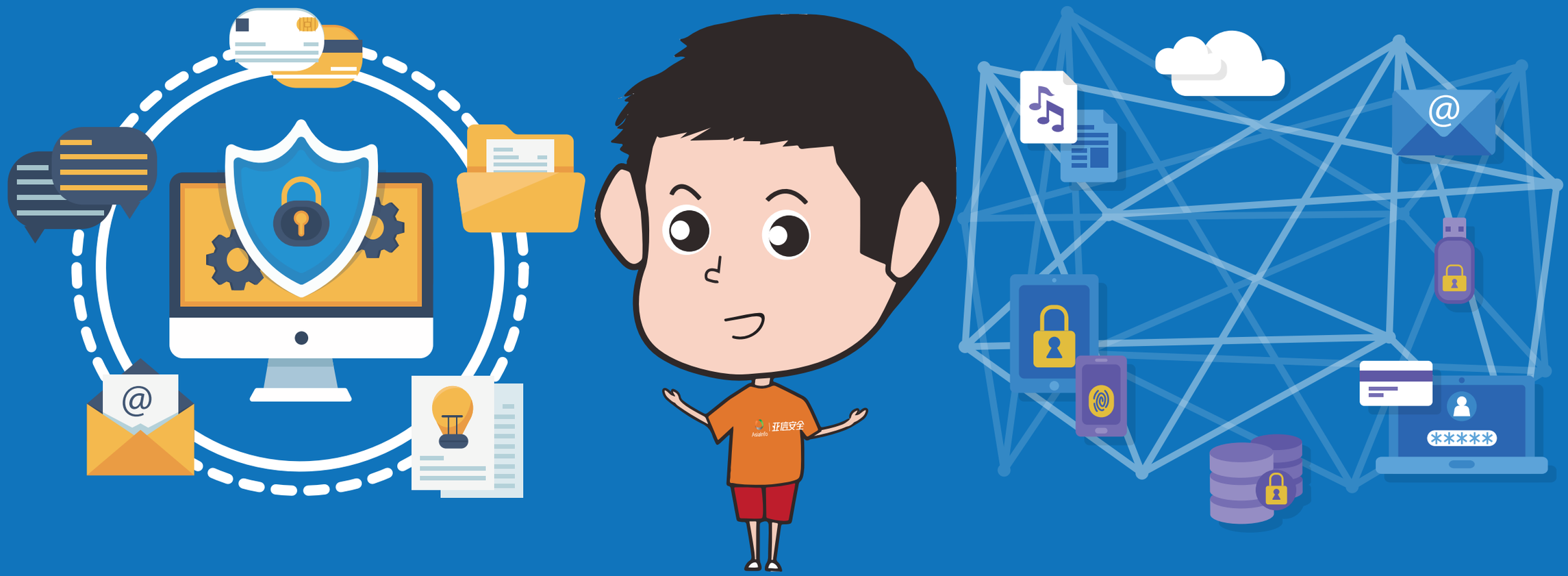
背景：疫情期间，为有效控制病毒传播、降低人员感染风险，全国大部分符合条件的企业现已进入远程办公模式，大家纷纷转战“线上”，通过网络持续开展各项日常工作。然而，当个人手机、家庭电脑和私人网络成为语音、文件等数据信息传输交换的主流途径时，你是否有意识到数据安全面临的威胁和风险？

从部署效率、成本、安全性这三个方面来衡量，公网直接发布虽然效率最快、成本最低，但其安全性也最差，而虚拟桌面虽然可以让企业获得最佳的安全防护效果，但很多企业根本无法在短时间内完成。因此，当前使用VPN连接方式和将内部一些应用发布至互联网上最为普遍，而安全问题也接踵而来。
纵观目前远程办公的安全问题，很多平台从未遇到过如此高的并发和负载，也因此导致了频繁出现严重延迟、卡顿或无法进入等意外情况，而在不能保障稳定性的情况下，安全性更令人担忧。

AsiaInfo | 亚信安全

远程办公时接入的认证安全

提供远程办公的基础架构安全



远程办公时接入的认证安全

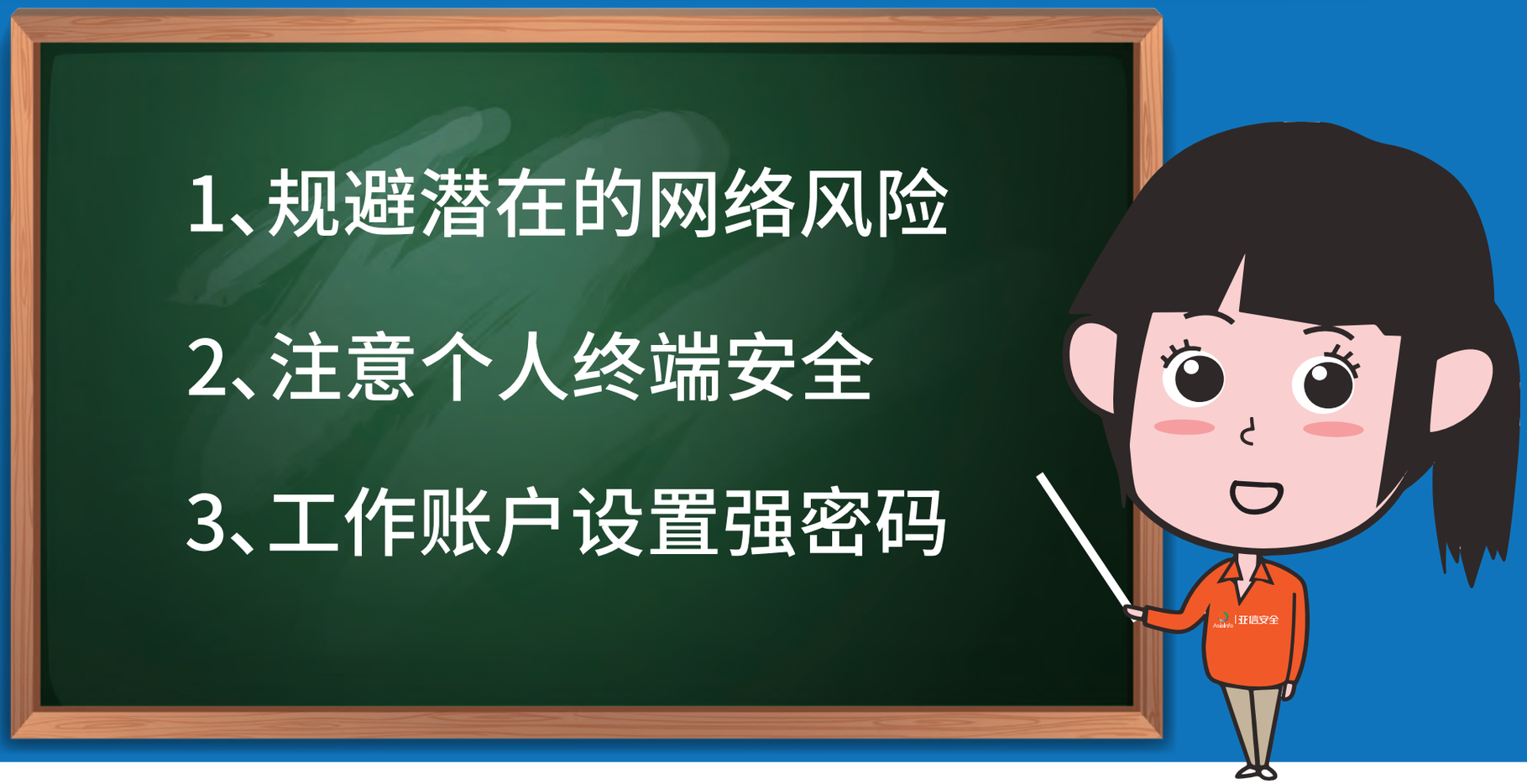
数据显示，盗用身份凭证仍然是黑客最常用、也是最有效的攻击和破坏手段（大约占81.1%）。这不仅包含了单一凭证登录时的密码复杂性问题，还包括了用户登录不同资源时会使用“同一密码”的情况，这增加了身份冒用、权限提升和数据信息泄露的风险。

提供远程办公的基础架构安全

另外一大类风险来自提供远程办公的基础架构，例如VPN自身设备、使用的TeamViewer、Zoom等远程协同办公软件是否安全，是否有漏洞，员工在家使用自己电脑设备是否感染病毒，被当成“跳板”攻击等问题，以及数据中心等核心架构可能遇到的恶意攻击。

AsiaInfo | 亚信安全

针对远程办公时数据安全防护的一些建议：



1. 在安装远程办公的软件之前，先看看有没有把WIFI密码泄露出去了，是否有人在蹭自己的网。远程办公会用到一些必备的软件和工具尽量确保在各大软件官网下载正版安装包。另外请保持使用的软件始终处于最新版本状态，及时下载更新补丁程序，其更新除了新增功能、体验优化之外，往往还伴随着安全漏洞的修复。

2. 在家远程办公期间，你可能会比以往更多的用到个人终端设备，它们不同于企业办公终端，没有专人统一维护，也更容易遭受黑客攻击或电脑病毒的感染，从而在使用过程中对数据安全造成意想不到的安全威胁。建议使用服务器深度安全防护系统 Deep Security、终端防护系统OfficeScan等软件解决方案可快速部署覆盖，对基础架构重要资源、客户端进行恶意软件检测查杀，其次虚拟补丁和IPS功能，可以保护内部重要资源免受各类攻击。

3. 确保登录账户密码的复杂度，建议大家在设置工作账户密码时，采用包含数字、大写字母、小写字母以及特殊字符组成的“强密码”，防止黑客通过撞库、爆破等方式入侵；在条件允许的情况下，强烈建议用户在VPN接入使用多因子认证或OTP。

AsiaInfo | 亚信安全

4、VPN使用建议

5、资源访问权限控制

6、内部资源共享安全

4. 在VPN接入认证时，建议用户接入前对接入客户端进行健康检测，检测接入客户端防病毒软件是否安装、病毒库版本是否最新等条件，如果满足条件则允许接入，不满足可以将接入客户端重定向到一个门户网站或者网盘，进行防病毒和其他必要软件的下载。

5. 远程办公人员常常需要将工作资料(包括企业文件、档案)等重要、敏感数据保存到个人终端设备上使用，如果没有严格的信息共享与保存准则约束，这种“使用”下的数据安全风险将难以估量。需要针对内网资源制定严格的远程访问权限和应用隔离，如果条件允许，启用远程访问用户的安全审计。

6. 如非迫不得已，尽量不采用资源发布访问模式提供远程办公，尽量减少资产在互联网上暴露，用户在将应用直接发布至互联网时，需要谨慎考虑安全性，例如不应该将3389、445等端口直接映射至互联网，这会减少被黑客扫描和攻击的可能性。不能确保终端安全的情况下，要尽量减少数据文件分发和共享，避免具备远程控制和窃取能力的感染型病毒在远程办公平台上传播。

AsiaInfo | 亚信安全

7、重要资料及时备份

8、注意钓鱼邮件及恶意网站

7.即便做好万全的准备工作也无法保证100%的安全，但在疫情期间很难做到“3-2-1”黄金备份法则。而远程办公中产生的数据也是企业生产的重要资产，所以应要求员工将重要文档、代码数据等采用云端和本地同时备份的方式，确保数据安全。同时请注意，除非已经过加密，否则切勿使用可能存在安全隐患的外部设备存储重要敏感数据。

8.疫情特殊时期，涌现出大量利用疫情相关信息命名的恶意软件或者钓鱼邮件，在家办公期间，尤其要注意那些未知来源的可疑电子邮件，切勿轻率打开或点击、下载其内的链接和附件，避免被诱导至钓鱼网站或感染各类电脑病毒造成数据泄露及一系列后续安全隐患。在遇到恶意引导下载软件时，一定要及时关闭浏览页面，遇到恶意弹窗建议可以直接断网。疫情过后，也要保持对公共场所WiFi、陌生蓝牙和共用USB设备等的安全防范意识。