远程办公网络安全意识培训

享安全

前言

随着互联网科技的发展，企业运营观念的改变，远程办公模式早已成为了众多企业的选择项。特别是在这次新型冠状病毒疫情的特殊时刻，让员工在家中安全地、即时地参与工作事务变成企业运营的关键需求，这也形成了史上最大规模的远程办公。

远程办公模式在为我们提供方便的同时，也带来了一些问题，其中安全性就是影响远程办公的重要因素之一， 加强远程办公网络安全常识宣传教育，提高员工的安全防范意识，掌握基本防护技能 ，成了确保远程办公网络安全的最基本条件。本课程选取多项网络安全意识教育内容，结合远程办公的特别场景，探讨人们如何在远程办公时保护企业数据安全与个人隐私安全。

目 录

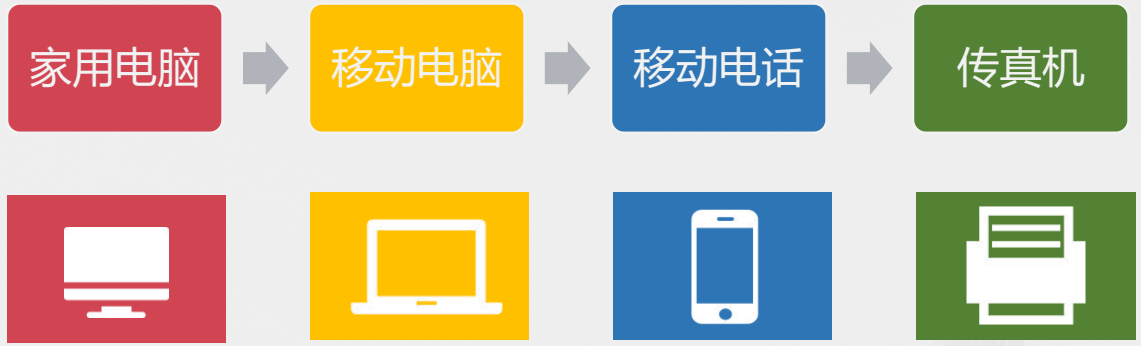
一

远程办公的特点

什么是远程办公

远程办公是指借助能够连接家用或公共网络的计算机，结合使用家用电脑、移动电脑、移动电话、传真机，并结合电子邮件、远程控制、音频视频会议软件等工具，在传统办公地点范围之外进行协同工作的新型办公方式。

最常见的形式便是我们熟悉的居家办公和差旅办公。

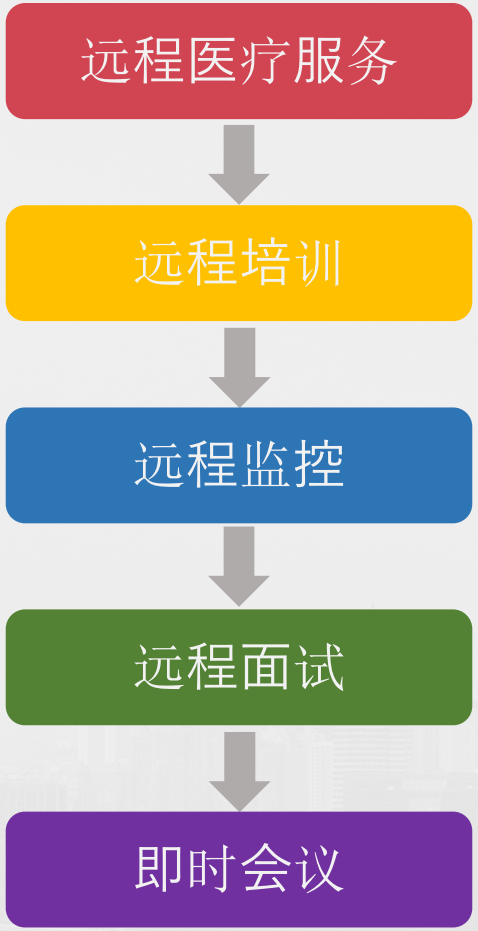


远程办公的优点

1、低成本，不受时空地域的限制。

2、场景应用丰富，除了传统的常规工作场景外，还可以实现诸如远程医疗服务、远程培训、远程监控、远程面试、即时会议等场景

3、高效、便利、自由，被认为是仅次于加薪的第二大员工激励，可以增加员工对公司的好感。



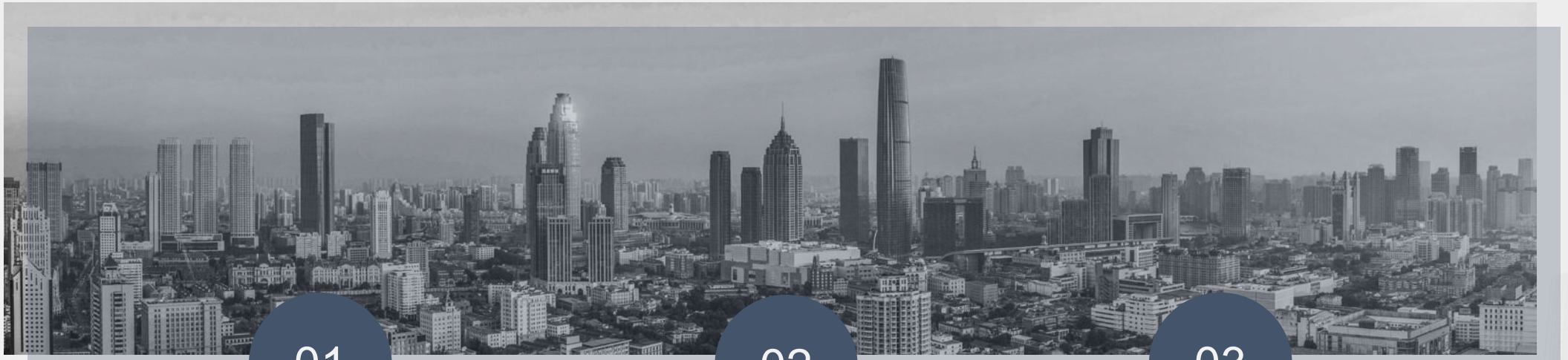
远程办公的缺点

没什么缺点，就是很不安全！

二

远程办公的环境安全

办公场所环境安全



01

住宅？酒店？商业和娱乐场所？交通工具？友商职场？室外环境等

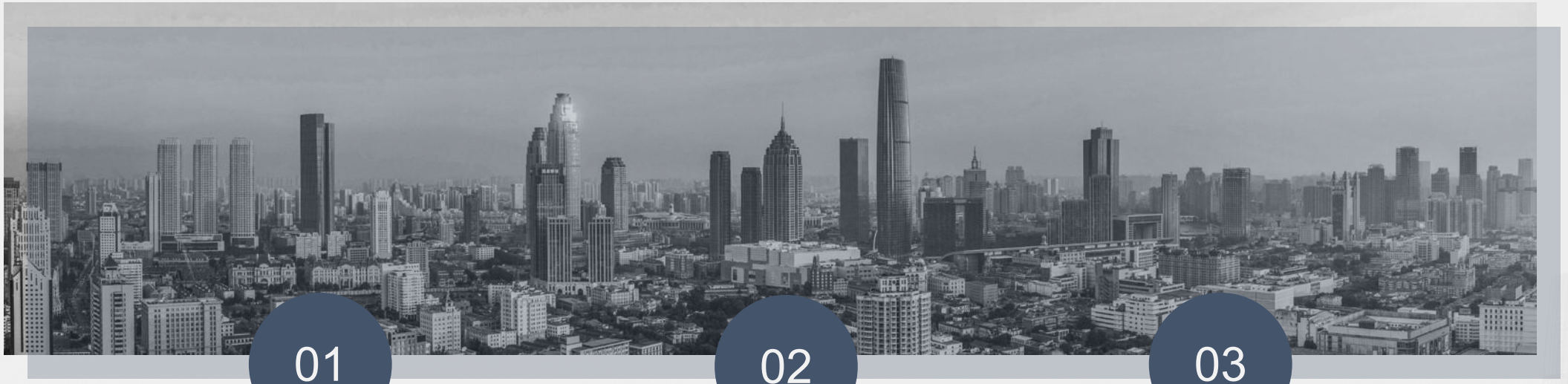
02

照明？供电？进出口等布局情况

03

家人？同事？陌生人？有儿童？

办公场所环境安全



01

偷窥？

咖啡厅等场所最容易发生偷窥。另外在家中也要留意家人因好奇而进行不必要的偷窥。

02

非授权操作

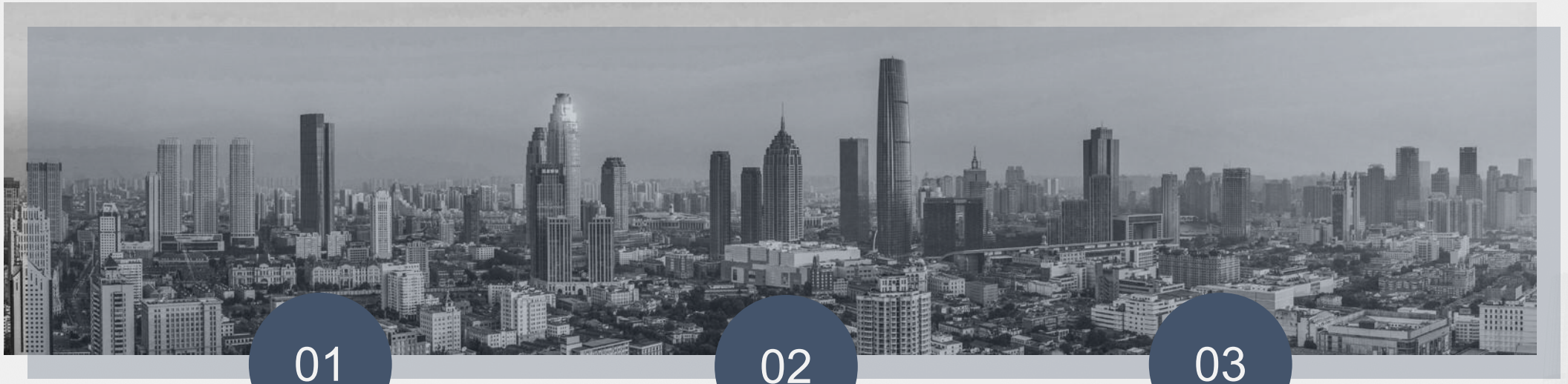
了解所处环境非授权操作的可能性，如防范儿童操作，避免造成出乎你意料的后果。

03

非法摄像、偷盗

了解所处环境被偷拍，偷盗的可能性，特别是在酒店房间等半公共场所。

局域网环境安全



01

内网攻击

了解网络的管理者，网络的用途，通过安全软件监控内网攻击、蹭网等情况。

02

文件共享

了解所处的局域网内共享设置，以免未授权的共享行为。

03

未知风险

解决一切未知风险的方法就是使可控已知的替代手段，请自备蜂窝网络工具或使用手机热点。

三

远程办公的终端安全

远程办公的终端安全

垃圾文件

流氓软件

蠕虫病毒

木马程序

WIN安全中心设置

控制面板设置

防毒软件

保持更新

区分办公与非办公系统用户帐户

远程办公的终端安全

与家用电脑、游戏、看剧、儿童学习终端区分

使用专门用于办公的U盘、移动硬盘

办公专用终端不连接家用充电宝、摄像头

自备蜂窝网络链接器，使用自身的手机热点

远程办公的终端安全

使用一台专门用于远程办公的手机或平板设备

将移动设备的系统与app保持版本最新相比计算机来说更重要

开源系统必须安装安全防护软件

仔细自定义关于相册、通讯录、信息、摄像头、麦克风、位置信息等隐私信息的授权设置

四

远程办公的软件安全

远程办公的软件安全

享安全

会议工具　解压缩软件　文档处理软件　远程控制软件

- 从公司正式渠道获得安装包与软件授权
- 从官网下载应用
- 绝不使用与远程办公无关的插件
- 根据需求自定义每个软件的详细设置

五

远程办公的口令安全

远程办公的口令安全

远程办公中，口令安全最大的问题是办公口令和生活口令混杂使用，这种情况使得口令安全环境更复杂，更容易滋生安全问题。

远程办公的口令安全

主动泄露

主动泄漏是指用户缺乏口令保护的安全意识，有意或者无意地告知、公布口令，被别有用心的人分析并利用。我们在远程办公时已留意杜绝这些行为。

1、上级委托下属处理带有审批权限的工作事务
2、女性员工最容易为便利主动交出口令
3、本地或云盘储存、发送、记录口令
4、将口令贴在键盘、显示器上

远程办公的口令安全

被动泄露指的是由于对口令的保护意识薄弱，口令设置与保护技巧缺乏，口令很容易被他人分析、猜测、破解并利用从而在不知情的情况下泄露。我们应该留意防范以下情况：

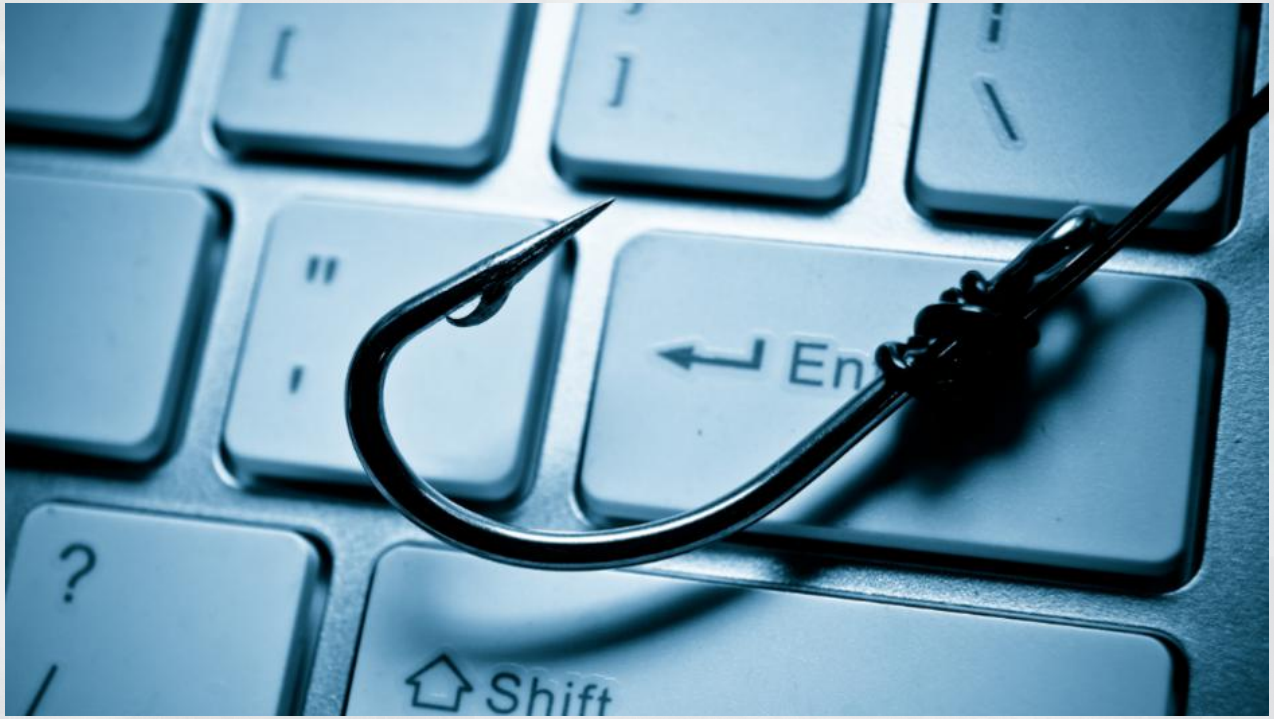
1、输入口令被偷窥
2、社会工程学攻击
3、口令设置简单或有较高关联性
4、口令重复使用

六

远程办公的邮件安全

远程办公的邮件安全

Business E-mail Compromise，也称作“CEO诈骗”，是一种具有高度针对性的鱼叉式网络钓鱼攻击。根据不同的场景，攻击者可能冒充企业的管理人员或者权威机构的内部人员，通过社会工程学方法获取被攻击者的敏感信息，并向指定的攻击目标发送商务性欺诈邮件。



远程办公的邮件安全

撒网式的钓鱼攻击往往是结合攻击对象所在的行业、公司或个人情况，以及社会关注事件等方面着手，发送引诱兴趣的邮件，往往通过具有欺骗性内容的附件、链接来引诱用户点击，从而获得办公终端的控制权限。

远程办公的邮件安全

使用企业邮箱帐号和应用

不直接回复可疑或重要的商业邮件

对于反常内容始终保持怀疑态度

使用专用的密码管理软件

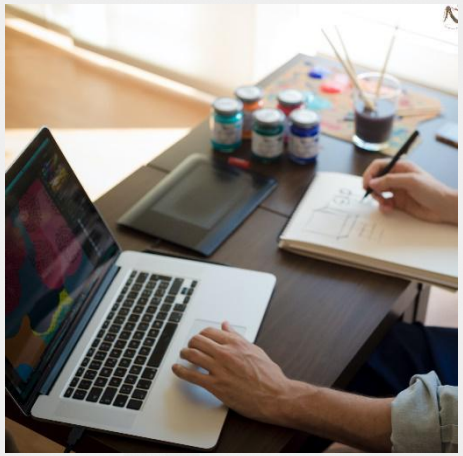
七

远程办公的数据安全

远程办公的数据安全

在远程办公的终端安全章节中，我们已经提到过要用专用的存储设备。在数据安全和数据备份层面，更建议大家对这些远程办公专用的存储设备加载额外的加密工具，相关的工具、原理与方法可以咨询公司的IT部门，这样可以防止他人拷贝你的文件，即便丢失存储设备也不用担心泄露公司机密和个人信息，当然即便做好了安全保护措施，我们依旧要防范存有办公数据的设备的丢失或被盗，建议可以锁在自己的钥匙上，或者放置在特定的带锁扣的袋子中。

设备专用



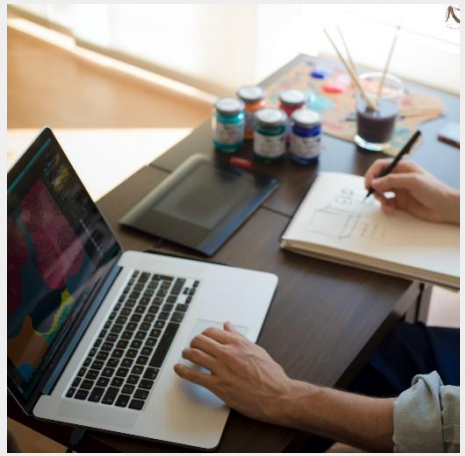
设备加密

设备保管

远程办公的数据安全

处理重要文档、代码数据等公司资产时记得随时备份，用加密的专用的 U 盘或者硬盘备份到本地专用的远程办公终端上，安全性便得到保障。部分企业对涉及企业机密信息或者代码会要求保存在内网存储，这也是比较安全可控的方式。对于现在流行的，将办公资料保存在云端上的做法，请咨询公司相关部门和了解相关政策，一定要保存在云端的，请使用公司合作的云服务提供商。

设备专用



设备加密

设备保管

八

远程办公的隐私保护

远程办公的隐私保护

选择封闭可控的办公环境，设置单调的背景，移除无关的物品

巧妙使用安全缓冲功能，如直播延迟、虚拟位置等

使用企业通讯软件交流和传输文件，不要使用微信、QQ等

关闭不需要的设备与功能，如摄像头，人离开便锁屏

九

远程办公的安全守则

远程办公的安全守则

- 不打开来历不明的电子邮件，不下载不明来源的文件
- 使用企业邮箱处理工作事务、杜绝在远程办公中使用个人邮箱
- 安装并记住更新杀毒软件程序和病毒特征库
- 不使用不安全的网络、如公共场所的免费WIFI等
- 学习和掌握本地安全设置，确保电脑、USB等设备加密

远程办公的安全守则

- 使用受信任的连接与证书，例如使用https，确保用户信息传输安全
- 确保只使用被授权的工作设备，包括电脑、U盘等
- 使用非企业即时通讯进行工作沟通时，避免涉及敏感信息，不传递重要资料
- 收到关于“新型冠状病毒疫情”等类似热点新闻的内容，不要随意点击链接及相关文件的下载
- 不要在朋友圈或其他社交媒体上发布工作相关内容

远程办公的安全守则

享安全

- 严禁在家开展涉密公务工作
- 严禁将　　、涉密计算机、涉密移动存储介质等带回家
- 严禁将涉密文件拍照存储于私人手机、相机等设备中带回家
- 严禁在普通手机通信中涉及涉密信息
- 严禁在私人计算机、存储设备中存储、处理涉密信息
- 严禁使用QQ、微信、邮件、网盘等存储、处理、传输涉密信息
- 严禁通过普通邮政、快递等无保密措施的渠道传递涉密信息
- 严禁未加密传输重要文件

谢谢！