疫情期间远程办公安全知识普及

天融信　　张超

目录

CONTENT

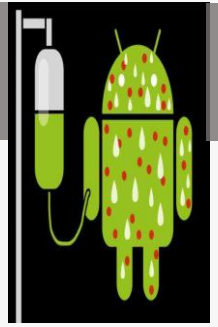
- 疫情期间远程办公方式及风险
- 安全建议及工具推荐

疫情期间远程办公方式及风险

设备风险
家用终端远程办公

1. 家人尤其是孩子误操作，可能影响重大
2. 重要数据在家用终端留存可能被各种渠道泄漏
3. 设备损坏、遗失造成数据泄露

人员风险
关键员工远程办公



1. 疫情爆发以来，欧洲、印度等国家黑客主动攻击我国网络。
2. 关键人员可能被定向网络攻击
3. 关键人员远程办公可能被监听

人员风险
一线员工远程办公

1. 一线员工的通讯内容不受约束，可能成为不良舆论源头
2. 一线员工的离职等情况，重要数据无法追回

钓鱼应用
通过远程办公发起攻击

1. 疫情期间个人公众号、网站信息繁杂，钓鱼链接盗取个人隐私甚至财产
2. 伪装办公APP推送，盗取账号后攻击远程办公网络

远程应用APP安全

1. 疫情期间，下载游戏APP可能被诈骗或诱导下载恶意APP
2. Teamviewer等远程桌面工具漏洞成为攻击跳板

远程网络安全
恶意WiFi

1. 个别超期返程员工，因家里没有WIFI或固定网络，个人4G套餐不足或耗尽，进而通过各种方式寻求免费WIFI热点，造成业务数据泄露
2. 公开无密码钓鱼wifi，劫持WIFI常开员工的网络连接

远程办公各阶段安全建议

尽量使用单位派发终端

如果一定要使用个人终端

1. 请安装杀毒软件的基础上
2. 尽量卸载个人应用
3. 使用单位派发安全工具办公
4. 添加锁屏密码/指纹认证环节

尽量使用家用加密WIFI或4G

如果流量耗尽可以跟单位申请流量费用

特殊情况下：

1. 验证网络能够访问公众网站
2. 安装杀毒软件或主机卫士
3. 传输重要数据或文件一定压缩加密
4. 登录办公后更换密码

办公应用一定从单位指定渠道下载

1. 无论单位派发或个人设备，都不安装非正规应用市场提供APP或WINDWOS安装包
2. 办公应用一定及时升级到最新版本
3. 不将单位办公APP或应用安装包外发

一定使用单位指定的办公工具

1. 从指定渠道下载办公工具，例如VPN客户端
2. 尽量不使用国外工具软件操作业务
3. 重要岗位使用具有安全功能工具
4. 办公工具升级到最新版本

尽量做到远程办公数据不落地

1. 有条件的情况尽量使用软件云桌面办公
2. 如果使用个人终端，下载的数据应加密存储或彻底删除
3. 移动端APP应在安全环境或加固后使用

提高个人职业素质及安全意识

1. 不信谣不传谣
2. 不将工作信息外传
3. 使用安全办公工具远程办公

常见远程办公工具分析

常见方案	好处与欠缺	解决方法
VPN方案 通过SSL-VPN远程办公 PC端最好配备USB-KEY做双因子认证。防止恶意操作或误操作	●方便、快捷，在PC端手机端都可以使用 ●数据传输加密，按权限访问内网业务 ●不涉及个人隐私，但是对办公终端业务数据防护能力有限	**●办公应用/手机APP加固** **●移动终端零数据留存，手机丢失也没有损失。** **●工作数据自动备份，可应对灾难风险。**
云平台SaaS服务 将业务或工具迁移到云端，使用公有云平台服务办公	●方便、快捷 ●工具本身的安全由云服务供应商负责 ●疫情期间客户业务服务器迁移困难 ●业务暴露在公网云端，公益受攻击 ●业务数据在云服务商平台存储，有泄露风险	**●使用已有的私有云提供服务** **●重要数据建议通过私有网络承载** **●一定要通过云端工具沟通，尽量不上传重要资料、通过公有即时通讯工具沟通涉密、与重大疫情相关信息**
云桌面方案 通过软件云桌面客户端访问公网云桌面虚拟机，进而访问真正的办公业务	●业务数据不落地，技术上杜绝数据泄露风险 ●传输数据为视频/图像，防中间人攻击 ●对终端的网络通讯及设备性能有要求 ●绝大多数国内厂家无法提供手机端云桌面	**●重要人员在处理重要数据的时候，建议使用云桌面办公** **●保证网络连接和设备性能** **●使用天融信手机云桌面产品**

常见远程办公工具分析

常见方案	好处与欠缺	解决方法
EMM方案 对一线移动智能终端强管控 实现远程定位、业务审计等功能 对丢失设备实现远程擦除	●派发设备能够被远程管理，丢失、人员离岗、盗窃等情况能够快速删除数据信息 ●能够对手机、执法PDA等智能设备上的APP提供安全工作域，保证移动办公业务安全 ●个人员工可能强烈反感个人手机被管被控	**●一线、重要岗位需要移动远程办公，建议使用企业派发设备，专机专用** **●建议与VPN配合使用**
远程桌面工具 类似向日葵、teamviewer 工具，使重要岗位远程办公好帮手	●个人免费、即开即用，减少人员聚集 ●适配性好 ●一次共享密码，认证后一直连接，存在风险 ●免费版漏洞更新不及时，数据被盗取 ●大型企业，对VPN性能压力暴增	**●非重要数据，可以实用** **●重要工作，即用即关，不建议长时间连接** **●一定及时升级到最新版本，有条件的情况，建议使用商用版本**

天融信远程办公　　非重要业务安全工具建议

SSLVPN（PC+移动端）建议必选，EMM+EDR（终端安全管理，选配）

远程办公终端

手机

Pad也可以哦

- ✓ 安全门户，提供极致移动工作体验
- ✓ 安全桌面，让终端变为专机专用

电脑

员工个人办公终端

- ✓ 安全门户，完全隔离企业数据和个人数据
- ✓ 移动数据防泄漏，全面保护终端业务数据

VPN隧道

- ✓ SSL-VPN隧道
- ✓ PC、移动终端病毒检测准入机制

远程内网办公平台

安卓私有推送

- ✓ 大数据可视化平台
- ✓ 分级分层管理

iOS云推送

- ✓ 全生命周期移动终端管理
- ✓ 企业级移动应用商店

PC+移动端远程办公通用解决方案

天融信远程办公　　重要业务安全工具建议

SSLVPN+云桌面（PC端+手机端）业务数据不落地、不泄露

安全 易用 方便 实惠

用户体验良好

近似真机体验，
无需任何权限。

传输安全

图像指令传输加密，
中间人攻击无效。

应用统一管理

统一管理，运维简单。

无需开发苹果应用

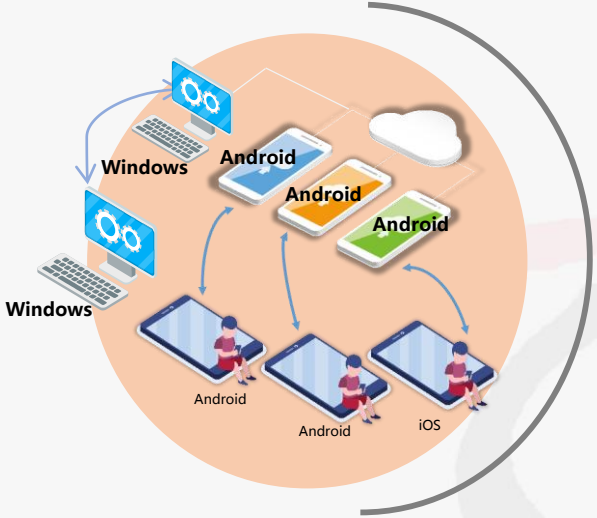
节约开发成本，无
需AppStore上架。

安全行为审计

截屏禁止&审计，
自动水印覆盖。

应用安全

APP无需漏扫加固，
真实业务内网访问，
业务数据不落地。



远程办公是一种临时办法，也可能是一种趋势。

无论什么时候了解其中的安全问题都很必要，这样才能在享受远程办公的便利同时，不会损失更重要的“财富”

感谢观看 祝大家身体健康