

法律动态

2020年5月

如需了解更多资讯，请联系以下人员：

Gary Seib
合伙人
+852 2846 2112
gary.seib@bakermckenzie.com

许峰
合伙人
+86 21 6105 5996
simon.hui@bakermckenzie.com

林之颖
资深律师
+852 2846 1686
gillian.lam@bakermckenzie.com

徐嘉铭
资深律师
+852 2846 2494
clement.chui@bakermckenzie.com

新冠疫情——当诈骗分子利用疫情进行网络钓鱼——降低在新冠疫情期间遭受网络诈骗的风险并最大程度地追回损失

随着全球经济因新冠疫情而放缓，世界各地的网络诈骗案件数量激增。自疫情爆发以来，香港警方、英国 Action Fraud（英国国家欺诈和网络犯罪统计中心）和澳大利亚网络安全中心所记录的与新冠疫情相关的网络诈骗案件数量均大幅增加。

从与采购个人防护装备相关的买卖欺诈，到最容易受到供应链中断影响的公司为目标的企业电子邮件黑客攻击事件——诈骗分子利用此次疫情所造成的恐慌心理和不确定性，在诈骗案件中展示出了高度成熟的技术和水平。网络诈骗会造成十分严重的后果，从而导致数千万美元/英镑/欧元的损失。

网络诈骗是一种数量庞大且瞬息万变的全球现象。我们的团队在香港和中国大陆已经成功处理了超过 100 起网络诈骗案件。本文将重点讨论由当前现状所引发的最新风险，以及我们如何帮助您追回资金和进行网络诈骗风险管理。

常见的网络诈骗类型

我们经常看到的几种网络诈骗类型包括：

- **首席执行官诈骗**——在这种情形下，个人（通常是财务团队中的个人）受到诈骗分子冒用公司高层的电子邮件（通常伴有电话沟通）施加的压力或误导，认为公司正在开展“高度保密”或“秘密”的交易，需要绕开常规内部控制流程完成资金支付，因而未经内控审核而将大笔资金转入诈骗分子指定的账户。
- **供应商诈骗或银行变更诈骗**——供应商的电子邮件被黑客入侵或模仿，从而误导受害人更改付款指令并向诈骗分子进行实际的支付。同样地，银行/金融机构也可能会收到来自“客户”的欺诈性邮件指令而做出错误的支付。
- **通过入侵复杂的系统直接窃取**——通常的情况是，诈骗分子入侵金融机构的系统，并假借银行现有客户的名义发布欺诈性的 SWIFT 指令，





将巨额资金转移至海外账户。银行可能只会在次日进行日常对账时才发现该操作的异常。

使公司/银行遭遇此类诈骗情形的突破口通常是，公司/银行员工无意中点击或下载了嵌入了恶意软件的链接或网络钓鱼邮件的附件。

新冠疫情所增加的风险

需要注意新冠疫情爆发所引发的各种新风险，例如：

- **假冒的供应商**——受害者为购买个人防护产品（例如消毒凝胶和口罩），而向假冒供应商的诈骗分子支付数百万美元的货款。
- **欺诈性慈善机构**——利用网络钓鱼电子邮件，冒充非政府卫生机构募集款项。
- **虚假的政府退税**——使用包含虚假政府退税信息的网络钓鱼邮件，引诱个人点击嵌入了恶意软件的链接（伪装成能获取退税资金的链接），从而向诈骗分子发送个人财务和税务信息。
- **其他有关“点击此处”的诈骗**——很多网络钓鱼诈骗的目的是从受害者处获取有价值的信息，从而利用这些信息获取经济利益或其他利益。常见的策略是，利用看似有可靠来源的（如非政府组织、医学专家或行业专家）关于治疗、疫苗、保护和预防措施或行业冲击的相关信息和专题信息，引诱个人点击链接或文件。一旦点击，系统将会自动下载恶意软件，使诈骗分子可以轻松访问存储在受害者电脑中的信息。

公司还需时刻保持警惕，对与各国政府最新发布的数十亿经济救助计划相关的潜在网络钓鱼诈骗提起注意。

我们会定期为客户提供一些实用贴士（如下文列举），以帮助客户降低卷入网络诈骗案件的风险，或在不幸遭遇网络诈骗时最大程度地追回损失。

- **迅速应对**——这对于最大程度追回损失至关重要：**(a)**通知您的银行,要求其撤销交易并通知收款银行退还或冻结相关资金；**(b)**报警；以及**(c)**与我们联系——我们可以采取包括提起诉讼在内的必要措施来追回资金。
- **培训员工和优化 IT 系统**——网络诈骗风险是瞬息万变的，企业需要开展有关网络诈骗风险的内部培训，并优化 IT 系统以防范最新的风险。我们可以帮助您准备培训，开展侧重于风险信号识别的真实案例研究，以及制定在发生可疑诈骗事件时应遵循的流程以最大程度地减少公司的损失。我们与网络服务供应商也有合作，可以通过模拟网络钓鱼测试和基准风险评估来测试网络安全措施的有效性。
- **合同和保险条款**——在进行合同谈判和评估保险条款的适宜性时，需要同时考虑网络诈骗的风险因素。例如：当供应商被黑客攻击时，由谁来承担相应的损失？
- **考虑监管义务**——除了财务损失以外，网络诈骗的主要后果还包括造成重要数据的丢失，以及引起监管机构不必要的关注。公司应当时刻



明确其所要承担的监管义务，例如数据保护、证券、货币及其他政府部门向其施加的义务。

新冠疫情正在改变我们的工作方式。在一个由技术驱动的世界中，这些前所未有的时代背景正在放大网络诈骗带来的风险。诈骗分子热衷于利用 IT 系统的漏洞和不可靠性牟利。尤其当人们远程工作时，诈骗行为更有可能无法被迅速识别。因此，公司必须做好充分的准备，以应对网络诈骗的冲击。

如果您对上述谈及的内容有任何疑问，或需要我们对任何问题进一步阐释，欢迎随时与您在贝克·麦坚时的联系人或本文所列出的律师联系。

www.bakermckenzie.com

北京市建国门外大街 1 号
中国国际贸易中心
国贸写字楼 2 座 3401 室 100004
电话: +86 10 6535 3800
传真: +86 10 6505 2309

香港鰂魚涌英皇道 979 號
太古坊 1 座 14 樓
电话: +852 2846 1888
传真: +852 2845 0476

上海市浦东世纪大道 88 号
金茂大厦 1601 室 200121
电话: +86 21 6105 8558
传真: +86 21 5047 0020

本刊物乃供贝克·麦坚时律师事务所的客户及专业人士参考之用。虽则本所已竭尽所能确保相关资料的准确性，本刊物并不是对所涉及的法律领域作出的详尽探讨，因而贝克·麦坚时律师事务所不对任何人根据本刊物中所包含内容而采取或规避的任何行动承担任何责任。若需针对个别问题的建议或其他专家协助，应向合资格的专业顾问寻求帮助。

©2020 贝克·麦坚时律师事务所，版权所有。贝克·麦坚时律师事务所是一家全球性律师事务所，作为其成员的律师事务所遍布全球各地。按照专业服务组织的通用术语，“合伙人”一词指上述律师事务所的合伙人或同等人员。同样，“办事处”一词指任何上述律师事务所的办事处。这可能构成“律师广告”材料，在某些司法管辖区可能因此需要作出通知。以前的成果并不保证将来会有类似的结果。