网络钓鱼诈骗防范指南

- 按照西得乐集团的财务会计管理政策，西得乐采用双重授权机制，对于付款指示的变更事宜也是如此。也就是说，任何此类变更，均需要“两位”已获西得乐法人实体授权的人员预先书面批准，方为有效。而且，这种变更付款指示的情况极为少见。西得乐很少会要求将付款接收行从一家银行变更为另一家银行，更不太可能变更到第三国银行。
- 西得乐的所有付款请求都会附带西得乐的发票。因此，如果付款请求没有附带正确的发票，应立即引起怀疑。
- 所有后续付款提醒或付款跟进查询，都会附带有关原始付款请求及发票的信息。如果付款请求中未附带该信息或附带的信息与原始付款请求或发票不符，应立即引起怀疑。
- 如果西得乐法人实体或代理人要求变更正常付款请求及付款指示，即便发件人看似来自西得乐，我们也建议您务必拨打常用的西得乐联系电话，致电您所信任的西得乐联系人，口头确认付款指示变更。**切勿**使用发件人在付款请求和付款指示变更中提供的联系方式。您应使用常用的西得乐联系号码，致电您信任的西得乐联系人，来核实具体情况。特别是，对于发送转账请求或要求提供业务敏感信息的电子邮件，如果其发件地址不是“名字.姓氏@sidel.com”这样的格式，请务必同相关人员口头核实。
- 西得乐只通过 sidel.com 邮件地址（例如，“名字.姓氏@sidel.com”这样格式的地址）与您沟通 。西得乐不使用任何其他以 sidel.net, side1.com, sidei.com 等结尾的邮件地址。
- 请勿打开或回复来自第三方的垃圾邮件。
- 请勿答复任何询问商业敏感信息或个人信息的电话或邮件信息。务必核对邮件来源（记录下原始付款请求中包含的具体信息，然后使用经过证实的联系号码回拨给指定人员）。
- 当通过电子邮件发送商业敏感信息时，请考虑对信息加密。
- 使用常用的搜索引擎访问网站时，应核对搜索引擎显示的 URL 地址，确认您要访问的网站是合法网站。
- 对通过电子通信方式（如电子邮件）与您沟通的任何人员，务必要核实其身份，如对其请求之目的有怀疑，也务必进行核实。
- 务必要提防包含网站访问链接的外部电子邮件，即便邮件内容貌似合理也要谨慎行事。
- 如果邮件内容或发件人可疑，请勿点击邮件中的超链接（如跳转到某个网页的链接）。如果邮件将您引到西得乐的网站，务请核实该网址是有效的 sidel.com 网址。
- 西得乐主要使用以下网站开展对外宣传：www.sidel.com, www.sidel.de, www.sidel.pt, www.sidel.es, www.sidel.cn, www.sidel.fr 和 www.sidel.ru。如果某封邮件要求您访问

其他的西得乐网站，请勿急于访问该链接，而是应先致电您在西得乐的相关联系人进行核实。

- 务必使用最新的安全修补程序更新电脑。操作系统（如 Windows）厂商也会定期提供安全增强程序，以提升操作系统的安全性。例如，Windows 允许用户通过 http://windowsupdate.microsoft.com 自动安装安全修补程序。
- 现在的互联网浏览器（如 Internet Explorer, Mozilla Firefox, Google Chrome, Safari (Apple) 等），菜单中都提供防欺诈网站保护机制和防网络钓鱼功能。您应定期将浏览器更新到最新版本。
- 电脑上的所有软件也应定期更新。软件厂商会定期向您的电脑推送更新消息，建议您更新他们的软件。
- 建议您安装防病毒软件以及防间谍软件（这两种软件功能经常通过同一个软件产品来提供）并确认是最新版本。这类软件也应当定期更新。
- 大多数防病毒软件依靠病毒数据库来查杀病毒，病毒数据库会频繁更新，甚至一天会更新数次。您可将防病毒软件设置成自动安装病毒数据库更新，以确保获得最佳的保护效果。建议您在安装或更新防病毒软件后对电脑进行扫描，以检查电脑是否感染了病毒。
- 建议您启动个人防火墙。这样可以保护电脑免受入侵，并对进出电脑的数据流进行控制。
- 保证您的电子邮件安全。您的电子邮件软件应配备垃圾邮件过滤功能。邮箱应设有登录名和安全性较高的密码进行保护。
- 如果怀疑您的电子邮件地址被盗用，请考虑使用新的电子邮件地址，并以适当方式将新邮件地址告知所有业务联系人。

最后，切记要反复核实任何有关变更转账或银行业务往来信息的请求，并核实授权发件人的身份。请使用常用的联系号码致电发件人来确认请求，而不要使用所收到的电子邮件中提供的联系号码。

要进一步了解相关信息，包括防欺诈的建议及指导，请访问全球专业支持网站 http://www.stopthinkconnect.org/和 http://www.antiphishing.org/来查阅相关内容。