BlackRock

# 网络和信息安全宣传

# 警惕诈骗和欺诈

当今世界，欺诈和诈骗无处不在。随着技术发展日新月异，为犯罪分子从世界上任何地方盯上您提供了更多便利。骗子会花时间研究受害者，他们所掌握的受害者信息往往比我们想象的还要多。他们利用受害者愿意相信他人的天性，与其建立融洽的关系。这些骗子可能富有魅力、善解人意，看起来知识渊博、有说服力。毕竟，他们只有花时间研究受害者并与其建立信任，才有可能成功实施诈骗。骗子的招数也变得越来越复杂，他们经常假冒贝莱德等知名公司，使其看起来正规合法，获取受害者信任。

# 骗子使用的招数包括：

## 钓鱼网站

伪造网站获取个人信息，然后利用这些信息与受害者取得联系，向其提供号称有吸引力的投资机会。

## 虚假个人信息

假冒监管机构网站上的真实员工姓名。

## 虚假电子邮件地址

利用免费的网页邮箱服务伪造电子邮件地址，或创建与真实公司类似的域名和电子邮件地址。

## 虚假文件

在投资说明书、申请表和交易信息等虚假文件上面，使用公司徽标和高层管理人员的照片，使其看起来正规合法。

## 时间压力

利用限时优惠、投资或机会，给您带来时间上的紧迫感。例如：如果您在本周末之前不进行投资，就会错失良机。

## 社交工程技巧

利用社交工程技巧（例如远程操纵），骗取机密或个人信息。

## 电子欺骗

骗子通过更改发件人姓名或号码，使信息、电子邮件或通话看起来像是来自正规公司的。

**因此，能够识别可能是骗局的预警征兆（或危险信号）至关重要。**

# 什么是预警征兆?

您能够发现表明您可能正在遭遇诈骗的潜在预警征兆或危险信号，这一点至关重要，以下是一些示例:

- 敬请留意，骗子要求您向与贝莱德没有明显联系的个人、公司或第三方的银行账户，通过加密货币或支付钱包进行付款。贝莱德绝不会要求支付此类款项。

- 请警惕那些高得似乎不真实而且与市场脱节的投资回报。

- 您要注意来自免费的网页邮箱或域名，且与正规邮件有细微差异的的电子邮件，如增减字母、数字或特殊字符（例如，包含多余字母 k 的 虚假电子邮件域名 blackrockk.com.cn，而不是正规的电子邮件域名 blackrock.com.cn）。请注意，贝莱德员工的个人电子邮件以 @blackrock.com.cn 结尾。

- 警惕在通讯过程中短时间内改变所使用的电子邮件域名（例如，先从 @blackrockbonds.com.cn 等虚假的域名发送电子邮件，然后再从 @blackrockbonds.co.uk 等不同的电子邮件地址发送）。在电子邮件会话中切换域名，可能表示旧的域名已被关闭且不再可用。

- 防范有人急切催促或威胁您做出紧急决定或付款，鼓励您投资，向您保证可以获得回报。

- 注意诈骗分子要求您支付新的或额外的款项，以获得已经进行的投资（假称出于税务、管理或其他目的）。贝莱德决不会要求您支付此类款项，来获得您的账户或投资。

- 骗子会提供限时优惠，逼迫您迅速做出决定或进行付款。

**请注意，该列表并不能涵盖所有情形。**

**如果有人突然联系您，而您对此有任何疑虑，请勿继续沟通。如果您觉得有压力，请在付款前先与您信任的人商量一下。**

# 诈骗和欺诈的类型

骗子可以利用多种渠道联系您，例如电话、短信、社交媒体、电子邮件甚至帖子。

## 1. 投资诈骗

骗子试图说服您投资不存在或毫无价值的东西。他们可能会突然联系您，或者您在搜索特定投资时输入个人联系方式后联系您。他们可能会先向您发送真实公司网站的链接，以获取您的信任，并声称是该公司的代表。他们甚至可能冒充该公司的真实员工。

**最新示例：**

- 固定利率债券诈骗，声称提供有保证的回报。我们看到其中有许多诈骗针对不同的金融机构，包括贝莱德。
- 数字货币投资诈骗，声称提供极具吸引力且有保证的回报。
- 虚假投资机会，由个人在交友或其他社交媒体应用程序或渠道上提供。

**投资诈骗的预警征兆可能包括：**

- 承诺保证获取高回报，并且几乎没有风险。
- 某人自称是大型知名公司员工或关联公司代表，主动与您联系。
- 施加压力，催促您立即投资。
- 使用类似知名公司的域名发送电子邮件。
- 未在金融监管机构注册的个人或实体。
- 在金融监管网站上已发布与您联系的个人或实体有关的警告。

## 2. 预付费欺诈

骗子要求您预付款项，并承诺您将获得价值更高的金钱、商品或服务（例如奖品、贷款、就业），但该许诺从未兑现。他们可能将款项描述为费用、佣金、税款或管理费用。

**最新示例：**

- 招聘诈骗：声称来自正规公司的员工可能会面试您，给您提供一份工作机会，然后要求您支付培训、背景调查或在家办公的设备的费用。敬请留意，贝莱德绝不会以提前付款作为雇佣条件。

- 您可能会被要求下载移动应用程序，或点击门户网站的链接以登录和投资，还可能被要求支付管理费或税费以创建账户。
- 为您提供低息或无息贷款的贷款诈骗，您必须在收到贷款收益之前预付款项（如管理费或手续费）。

**预付费欺诈的预警征兆可能包括:**

- 以进行下一步或合同条件为借口要求必要的付款。
- 要求您支付费用，以获得已经进行的“投资”。

## 3. 社交媒体诈骗

骗子以贝莱德等正规公司的名义，或冒充该公司的员工或关联公司代表，建立虚假的社交媒体账户（如 LinkedIn、微信等）。他们可能会利用这些渠道与您建立联系，并对您实施诈骗。为了看起来更正规，他们可能有庞大的社交网，其中或许包括他们假冒身份的所在公司的真实员工。警惕未知联系人通过这些渠道向您提供的机会！

**最新示例:**

- 伪造的 LinkedIn 个人资料，声称是贝莱德的员工（首席执行官，部门负责人）。
- 通过社交媒体平台提供的数字货币投资诈骗。

**社交媒体诈骗的预警征兆可能包括:**

- 在社交媒体上，收到陌生人来路不明的信息，声称可以提供高回报。
- 在社交媒体个人资料页面，声称担任大公司高级管理职位，可以直接接触投资机会。

## 4. 身份盗窃和欺诈

身份盗窃是指骗子获得很多关于您的个人信息（如出生日期、全名、历史地址记录、税务号），并利用这些信息实施欺诈。他们可能会拦截您发布的帖子、电子邮件，以获取这些信息，或从互联网或暗网上收集有关您的数据。身份欺诈是指骗子利用您被盗的身份欺骗他人，以获取商品或服务。这方面的例子包括开立银行账户、接管现有账户（银行/投资）、以您的名义订购商品/服务。

**最新示例:**

- 虚假的投资账户、贷款或信用卡申请

**身份盗窃和欺诈的预警征兆可能包括:**

- 有人突然给您打电话，要求您通过电话提供个人信息。

- 向您发送网站链接，尤其是在您收到意料之外的链接的情况下要求提供个人信息。

## 5. 账户盗用欺诈

账户盗用欺诈是指骗子在未经授权的情形下，利用您的个人信息访问您的投资或银行账户，并将款项转移到他们控制的欺诈账户。他们可能会通过拦截您发布的帖子、电子邮件、收集互联网和暗网上关于您的可用数据，或您可能无意中提供的数据，以充分获取您的账户信息。

**最新示例：**

- 骗子冒充金融机构客服，要求赎回和更改银行账户。

**账户盗用欺诈的预警征兆可能包括：**

- 您收到有关更改账户的电子邮件或通知，但您之前没有进行任何更改。
- 您注意到账户中有未经授权的付款。

## 6. 商业邮件欺诈或付款转移欺诈

商业邮件欺诈（也称为付款转移欺诈或授权欺诈）是指骗子冒充企业熟悉的公司或个人向该企业发送电子邮件。然后，骗子会要求付款或通知企业银行账户详细信息发生了变化，以将企业付款转移到骗子控制的银行账户。为了看起来更正规合法，骗子可能会创建虚假电子邮件地址，该地址与他们试图冒充的电子邮件地址非常相似，比如通过增减或替换字母（例如，@blackrock.com.cn 对比 @black**k**rock.com.cn），并且可能会伪造发票或发送虚假发票。

**最新示例：**

- 骗子访问供应商的电子邮件账户，并通过该账户发送一封电子邮件，表示他们已经更新了发票付款的银行详细信息，希望该企业更新该虚假信息。骗子更改“回复”地址，以确保他们收到企业的任何回复。
- 冒充公司首席执行官向员工发送电子邮件，要求向骗子控制的账户紧急付款。

**商业邮件欺诈的预警征兆可能包括：**

- 电子邮件地址和域名的细微更改。
- “回复”地址与发件人地址不一致。
- 紧急要求付款。
- 出于保密原因，要求不与任何其他人进行交流。

# 保护自己免受诈骗和欺诈

请始终保持谨慎，警惕欺诈或诈骗风险，尤其是在付款之前。以下是一些关于如何保护您的钱财和个人信息的提示：

## 牢记要点：

- 保持警惕，切勿轻信别人告诉您的信息。对于不确定的事情，切勿继续。注意潜在的预警征兆。
- 在做出决定之前，请与您信任的人商量，或拨打可信来源的电话号码（切勿使用发送给您的文档上的电话号码）。
- 在您的设备上安装杀毒软件，并确保您的手机和平板电脑已更新到最新的操作系统版本。
- 及时销毁和您金融投资有关的信息，不要随意丢弃。

## 注意事项：

- 切勿将您的个人信息（例如银行详细信息、PIN 码和密码）透露给突然与您联系的任何人。
- 切勿因为被人催促而急忙付款。
- 切勿点击意料之外收到的电子邮件或消息中的链接。犯罪分子可能会利用此招数来访问您的电脑系统。.
- 对于突然与您通话的人，切勿允许其远程访问您的电脑或任何其他设备。

# 如果我被骗了，该怎么办？

如果您感觉自己被骗了，并且受到了金钱损失，我们建议您采取以下步骤：

## 1. 联系银行

立即联系您的银行。他们或许可以停止或收回付款。

## 2. 向执法部门报告.

向您所在司法管辖区的执法部门报告。

## 3. 向金融监管机构报告.

请向您所在司法管辖区的金融监管机构报告（如适用）。