# 防钓鱼式诈骗

中职一年级

## 本章学习目标

1. 能正确阐述钓鱼诈骗定义
2. 能辨别钓鱼诈骗的伎俩及手段
3.能采用正确方式防范钓鱼诈骗

家住安徽的小宁正准备睡觉，却在不到1分钟的时间里，收到了一个接一个的银行扣款信息，金额加起来有近11万元，瞬间把她吓得睡意全无！小宁到底遭遇了什么？是谁盗走了她银行卡里的积蓄？事情还得从那天小宁的一次购物交易说起。

小宁在网上选中了一条标价为279元的裙子，讨价还价后卖家同意以200元的价格将衣服卖给她。付款成功后，小宁收到了

银行发来的成功扣款的信息。但是随后，一个自称卖家的人，却打电话来告诉她，付款并未成功，并告知小宁，“订单出现了异常，联系订单处理中心吧”。随后，给小宁发了一个订单处理中心的QQ号码。

小宁对这个“卖家”的电话并没有过多怀疑，便添加了这个所谓的订单处理中心的QQ。将情况告知后，对方很快提出了解决方案，询问小宁购买衣服时所付款的银行，并发来了一个网址，告知小宁须10分钟内处理解冻程序，不然200元的损失将无法追回。

在对方的一再催促之下，小宁点击了链接，发现的确是她付款所用银行的网站，便放松了警惕，依照提示输入了身份证号、银行卡密码和验证码，等待自己“异常订单” 的解冻。

她的手机很快就收到了短信通知，然而，她收到的不是退款信息，而是扣款信息。这时，小宁确认自己是受骗了，于是立刻报了警。

思考：1、小宁为什么会上当受骗？

2、生活中还听说哪些类似的诈骗案例？

# 一、钓鱼诈骗定义

钓鱼诈骗又称钓鱼式欺诈，是指利用虚假网站窃取用户的银行账号及相关资料，进而达到非法窃取其资金的目的。钓鱼式欺诈目前在社会上时有发生，变化也越来越多。在钓鱼式欺诈活动中，犯罪分子发送虚假电子邮件或模仿可信赖的网站，目的是诱骗公众在虚假网站上输入银行账户登录信息或其他个人资料，达到攫取公众财产的目的。

# 二、常见的钓鱼诈骗伎俩

## （一）假冒购物网站

不法分子首先建立一个假的购物网站，然后在淘宝网、腾讯网等支付平台发布虚假的商品信息，该信息中的商品价格往往比市场同类商品便宜很多，同时不法分子还会留下自己的QQ号或者微信号等即时通信工具号码以及假购物网站的网址。当客户对该网站销售的便宜商品动心，并通过该网站购物进行支付时，就会链接到一个假的银行支付页面，客户在假支付页面输入的卡号、密码等信息就会被不法分子获取。

# 二、常见的钓鱼诈骗伎俩

## （二）假冒银行网站

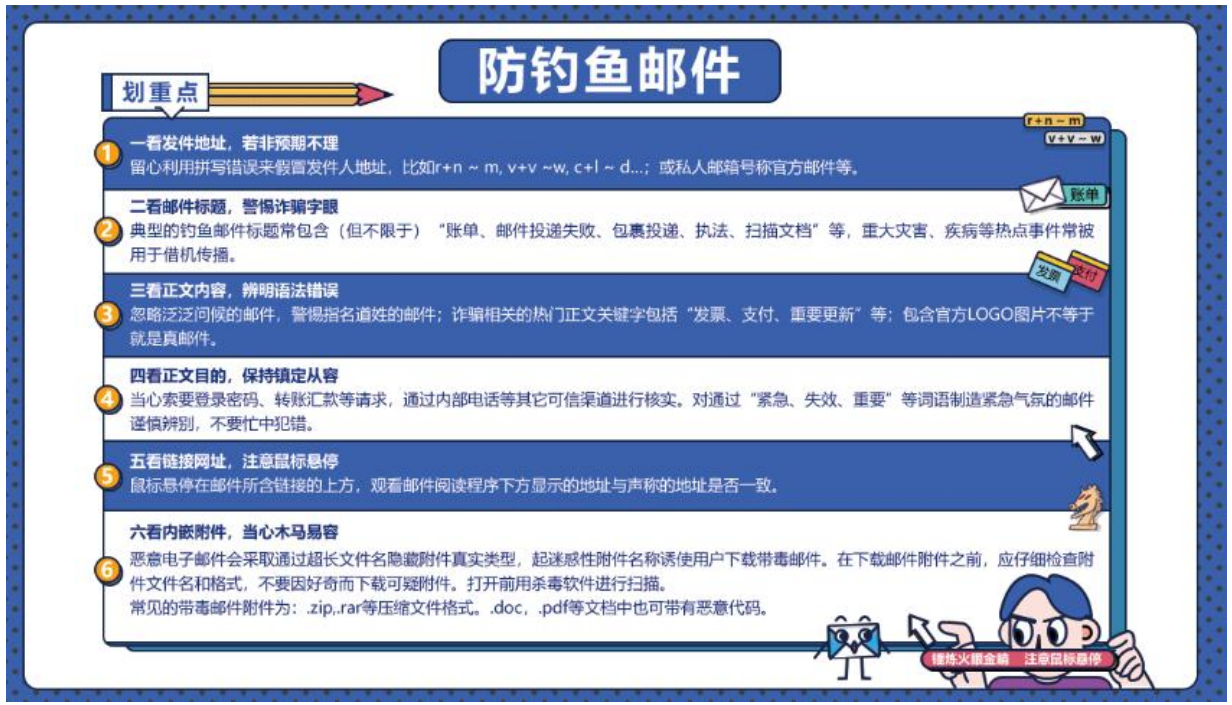
不法分子在网络上设置与真银行网站域名相似或外观相似的站点，诱骗客户输入用户名及口令，盗取信息后进行网银转账。

此外，钓鱼网站往往还通过伪基站短信群发扩散其地址、引诱用户点击，从而钓取用户的个人信息、银行卡卡号和密码。其中，中奖类钓鱼网站一般通过短信、微信或淘宝旺旺等方式传播。值得注意的是，一旦用户点击登录中奖钓鱼网站并填写个人信息，不法分子还会实施进一步的诈骗步骤，通过假冒公检法机构以法院传票等方式继续威胁、忍吓用户，从而实施诈骗。

# 二、常见的钓鱼诈骗伎俩

## （三）垃圾邮件

不法分子以垃圾邮件的形式大量发送欺诈性邮件，这些邮件多以中奖、顾问、对账等内容，或是以银行账号被冻结、银行系统升级等各种理由，要求收件人点击邮件上的链接地址，登录一个酷似银行网页的界面，而用户一旦在这个指定的登录界面输入了自己的卡（账）号、密码等，这些信息就会被窃取，最终被骗取账户资金。



# 二、常见的钓鱼诈骗伎俩

## （四）木马程序

不法分子通过木马程序等网络技术手段或其他手段，远程操纵客户电脑获取客户密码等认证信息，从而盗用客户资金。不法分子一般的做法是在发送的电子邮件、短信、QQ、微言、微博或网站中 藏“木马”程序，用户使用电脑或手机时不慎点击邮件或信息，或者浏览这些网站，就会感染“木马”病毒。用户在感染“木马’病毒的电脑或者手机上进行网上交易时，“木马”程序就会以键盘记录的方式获取用户账和密码，最终导致财产损失。

# 三、防范钓鱼诈骗的方法

（一）登录正规网站

当需要在电脑或者手机上登录和访问网站时，首先，要注意核对网址的真实性，在访问重要的网站时最好能记住其网络域名或者IP地址，确保登录到正确的网站，避免点击搜索引擎搜索出的链接。其次，要养成良好的使用习惯，不要轻易登录访问陌生网站、黄色网站和有黑客嫌疑的网站，拒绝下载安装不明来历的软件，拒绝可疑的邮件，及时退出交易程序，做好交易记录并及时核对等。

# 三、防范钓鱼诈骗的方法

（二）谨慎点击不明链接

我们要有自我保护意识，上网时谨慎点击不明链接，陌生人发送的链接或者下载的非官方软件一定不要点击。

如果手机、QQ、微信等收到不明链接，应采取“不予理睬”的态度，不点击、不查看，避免上当受骗。此外，智能手机和网银用户要对手机定期杀毒，各种银行卡、支付宝转账要通过官方网站下载的App软件进行操作。

# 三、防范钓鱼诈骗的方法

（三）注意保护自己的隐私信息

很多银行为了保障用户的安全，妥善保管用户的个人信虑资料，设定了登录密码（查询密码）和支付密码（取款密码）两套密码。用户若保证登录密码与支付密码不相同，即使登录密码被窃取，网络钓鱼者依然无法操作用户的资金。尽量选择安全的密码，建议选用字母、数字混合的方式，以提高密码猜测和破解的难度。密码等个人资料应妥善保管并定期更新，避免将密码泄露给他人。此外，还要特别注意身份证、银行卡等证件信息以及手机号码的妥善保管。

## 八种行为容易泄露个人隐私：

1、网络购物要谨慎钓鱼网站。

2、妥善处置快递单、车票、购物小票等包含个人信息的单据。

3、身份证复印上要写明用途。

4、简历只提供必要信息。

5、不在微博、群聊中透露个人信息。

6、慎在微信中晒照片。

7、慎重参加网上调查活动。

8、免费WIFI易泄露隐私

## 五类要警惕的钓鱼网站

1.假冒银行。案例一一尊敬的建行用户：您在我行账户已满10000积分，可免换5%的现金，请用手机登录www.ccbsell.com查询兑换，逾期无效【建设银行】。

2.假冒电信运管商。案例——尊敬的用户您好，您当前拥有4653积分即将过期！可兑换426元现金礼包！请登录10086jfm-zj.pw，按提示激活领取！【中国移动】。

3.假冒某热门栏目。案例——恭贺您成为《奔跑吧兄弟》场外幸运星。得到180000元及笔记本电脑一合，请点击22J5v3.net查领；验证码【9245】。

## 五类要警惕的钓鱼网站

4. 假冒购物网站。案例——尊敬的手机用户您好！您的手机号已被淘宝网13周年感恩大回馈、梦想创业基金活动组随机抽选成为幸运二等奖用户，您将获得淘宝网与赞助商提供的二等奖奖金260000元与苹果MacBookPro笔记本电脑一部！详情请登录活动网：【tbexy.CC】领取您的奖项，您的验证码为：【5168】，本次活动已通过公证处审批，请按照活动程序办理领取工作。

5. 假冒某公司。案例——尊敬的Apple用户：您好！您丢失的Iphone设备正在向官网申请激活设备，此人身份不符。请登录www.apple.ifogt.com拦截。拦截成功后将定位此设备，并与您取得联系，如您未丢此设备请忽略本信息，我们将在24小时后默认激活此设备【Apple安全中心】

# 谢谢大家