“尊敬的用户:我行网站已升级,请您尽快登录网上银行www.boccp.com进行动态密码维护,以确保您的资金安全。”近日,多位读者向本报记者反映收到了网络银行诈骗短信。专家表示,临近岁末,网上银行诈骗短信呈多发趋势,各类骗术层出不穷,市民应提高警惕。

读者秦女士表示,她收到上述短信的落款为“中国银行”。“我确实有中行账户,所以就按照短信提示打开了网址。”该网站与她以往所登录的银行页面布局一致。“不过这条短信是一个手机号码发送的,而不是中行的客服95566。所以我留了个心眼,通过网络搜索引擎重新打开了中行网址,这才发现两个地址是不一样的。”

记者注意到,短信中的“www.boccp.com”与真正的银行网站的网络地址“www.boc.cn”很相似,不仔细辨别很难发现。而且,该网站与正牌的中国银行网站的页面设置、内容基本一致。专家表示,不法分子通常会制作高度仿真银行网页,再群发虚假短信,并提供该网址,引人注意,一旦用户上网输入用户名和密码,犯罪嫌疑人就可以从网页上窃取账户名和密码,转移受害人卡内存款。

更具有讽刺意味的是,记者还在该钓鱼网站的首页上发现了一条名为《关于防范短信等方式欺骗客户登录钓鱼网站的安全提示》的公告,以显示自己的“正牌”地位。公告称,近期接到客户反映,有不法分子通过短信等方式发布欺诈信息,以“系统升级”或“动态口令过期需进行信息维护”等为由,诱骗客户登录假冒网站,骗取客户网银用户名、密码及动态口令,盗取客户账户资金。提醒广大客户增强安全意识,不要相信不明来源的邮件、短信和电话。

无独有偶,读者刘先生最近也碰到了相似的事情。他在某信用卡论坛发现了一个“提高信用额度”的帖子,并保证100%成功,提高额度后收费。刘先生在提供卡片相关信息后,负责提额的中介表示,他的信息已经提交到银行,银行信用卡中心会打电话确认提额的事情。

此后,刘先生接到银行信用卡中心的确认电话,并支付了中介手续费。但他在消费时却发现额度根本没有提高。业内人士表示,问题就出在这个信用卡中心的电话上,现在有一种网络电话,在使用这种网络电话拨打电话的时候,可以让对方的来电显示上显示任意号码,骗子们就是利用这种网络电话冒充信用卡中心的工作人员告诉刘先生提额成功,事实上根本没有这回事。

每年年底,手机短信诈骗都层出不穷。为此中国银联有关专家表示,要熟悉各家银行的客服中心电话,不要轻易相信其他电话号码发来的“风险提示”。对可疑的语音电话或短信不要回应,应直接致电相关单位或发卡银行客服热线询问,并登录正确的网

上银行网站。直接在浏览器中输入银行网站地址进入网站页面,并将该网址添加至收藏夹,方便下次使用。不要通过其他网站链接访问网银网站。如果发现仿冒银行网站,请立即向银行举报。