

记者 张国桐

“交管12123提醒：您的高速E卡已被限制使用。”近日，有不少车主收到这么一条来自“交管12123”的短信。根据短信内容显示，车主需登陆网址签署文件，若按期未签署文件，车主的高速E卡将被清除。

8月22日，记者从警方获悉，此短信是电信网络诈骗分子骗取钱财的新方式。虽然说是新方式，但该诈骗方式本质“换汤不换药”，依旧是ETC类诈骗。如果车主信以为真，点开短信里的网址，那么，就一步步掉入了电信网络诈骗分子的圈套。

说起最近出现的新型ETC电信网络诈骗，8月22日，济南市公安局历城区分局反诈中心负责人王成林表示，这些短信都是诈骗分子发送的虚假ETC短信，一旦车主填写了个人信息和银行账户密码，钱就可能在不知不觉中被转走了。

“诈骗分子群发短信，把车主作为目标，借助交管12123或高速企业的知名度，从而让车主上当受骗。”王成林说，该新型电信网络诈骗本质上依旧是ETC诈骗，只不过诈骗分子更新了伪装，以交管12123的名义，打着ETC异常的幌子，让车主自行走进骗子设下的陷阱中。

王成林表示，在车主的手机收到这种开头为“交管12123”或“高速ETC”的虚假短信提示后，警惕性不强的车主就会认为自己的ETC存在异常情况。之后，为了解除异常，车主便会点击短信内附带的“网站链接”。

“实际上这些网站都是骗子设的虚假网站。在网站内，骗子会按照设定的套路，让车主依次填写个人信息、银行卡信息等，车主一旦填写，银行账户内的钱就可能被骗子盗刷。”

由于短信具有迷惑性，很多车主在收到短信后，没细想，没核实，就直接点击链接操作，结果导致被骗。

那么，这种类型的诈骗方式，有何破解之策？对此，王成林表示，这种类型的诈骗方式骗取的金额相对较小，而且诈骗方式也比较容易识破。“在收到短信后，只要车主能冷静思考，及时核实自己ETC的情况，这种骗局就不攻自破了。”

对于不明号码发送的短信内容，市民们要提高警惕，加以核实。例如，收到交管12123短信后，可拨打全国统一交管服务热线电话12123或到银行营业网点核实短信内容真伪。

短信内

附带的链接，

骗子很可能在链接内设下了

能自动获取手机最高权限的木马病毒等，从而盗刷市民银行账户中的钱财。

“这种陌生链接千万不要点击，涉及重要个人信息、银行卡信息输入，特别是要求填写银行卡密码和验证码时，市民要多留心眼。”王成林说。

其实，无论何种类型的骗术，何种方式的伪装，骗子的目的从未改变，那就是骗取钱财。因此，市民切勿相信天上掉馅饼的事，提高防骗意识和警惕性，不给骗子留下可乘之机。