**绷紧防范之弦 远离诈骗之害**

**How to Stay Away From and Guard Against Scams**

全体师生：

年终岁尾，又到了电信诈骗的高发期。接警方数据统计，今年我校师生电信诈骗案持续呈高发态势，案件高达25宗，受骗金额累计接近100万，位居高新区高校排名第二，这个数据实属惊人。信息时代套路多，诈骗手段在发展，大家要想不上当，防骗指南看一看。

**诈骗手段可归纳为四类：**

亲情类：QQ借钱、短信催款、网络交友

恐吓类：冒充公检法人员、冒充黑社会、冒充公司老板要求汇款

名利类：刷单、兼职招工、中奖、低息贷款、购车购房退税

购物类：商品质量问题退款、海关扣押退款、取消绑定服务、购买演唱会门票

**防诈骗要做到“六个一律”，“八个凡是”，“一个确保”：**

**六个一律**

只要一谈到银行卡，一律挂掉；

只要一谈到中奖，一律挂掉；

只要一谈到“电话转接任何执法机构”，一律挂掉；

所有短信，需要点击链接的，一律删掉；

微信上不认识的人发来的链接，一律不点；

一提到“安全账户”的，一律是诈骗。

**八个凡是**

凡是自称任何执法机构要求汇款的；

凡是叫你汇款到“安全账户”的；

凡是通知中奖、领奖要你先交钱的；

凡是通知“家属”出事要先汇款的；

凡是在电话中索要银行卡信息及验证码的；

凡是让你开通网银接受检查的；

凡是自称老板或者领导要求汇款的；

凡是取消代理业务、扫二维码退款的；

一律不予理睬。

**一个确保**

确保下载了“国家反诈中心APP”，根据提示实名注册，**开启诈骗预警*。***当手机收到涉嫌诈骗的电话、短信或者下载安装了涉嫌诈骗的APP时，可以智能识别骗子身份并及时预警提示，极大降低受骗可能性。

还没下载的老师、同学们，请尽快扫码下载：

****** 

*别以为骗子离我们很远，其实时刻在身边，再不警觉加强自我防范，被骗的或许下一个就是你了*。

Dear staff and students,

As the year draws to a close, we are approaching the peak period for telecom scams. According to police statistics, such frauds targeting our staff and students this year are on the upward trend, totaling 25 cases in all, amounting to almost one million yuan in value. This puts us in the no. 2 spot among the higher education sector in the Hi-Tech Zone for the number of scams recorded. These numbers are a cause for alarm. The digital age has produced a multitude of online scams, and new schemes are being hatched all the time. Forewarned is forearmed.

Broadly speaking, telecom scams can be classified into **4 categories:**

1. Relationship scams—soliciting loans on qq. short messages demanding cash and online dating

2. Threats or intimidations—posing as law enforcement officials, or underworld gangsters or company bosses demanding cash transfers

3. Fake transactions—phony deals, offers of part-time employment, prize scams, low-interest loans, tax rebates involving real estate or car purchase

4. Shopping—refunds on defective goods, refunds on goods seized or detained by customs authorities, cancellation of binding service contracts, or purchase of concert tickets

**6 Red Flags:**

1. Any mention of bank cards, hang up

2. Any mention of prizes won, hang up

3. Any mention of calls connected to law enforcement, hang up

4. Any short message requiring you to click into a link, hang up

5. Any links sent by unknown persons, don’t click

6. Any mention of account security can only be a scam

**8 Don’ts:**

1. Any calls claiming to be from law enforcement demanding transfer of funds

2. Any calls asking you to remit funds to a “secure account”

3. Any notification of you having won a prize but asking you to first pay a handling fee

4. Any claims of a family member in distress or danger, demanding a cash rescue

5. Any calls asking for your bank information or password

6. Any request for your online banking to be open to investigation

7. Anyone claiming to be a boss or leader instructing you to make transfer of funds

8. Any cancellation of agency service that requires the scanning of a QR code for a refund

**1 Do:**

Download the National Anti-Scam Center APP, by using your real name for registration. When you receive a suspicious call or message, open the Scam Alert to detect the identity of the scammer. This will substantially reduce the possibility of being scammed.

We urge teachers and students who have not yet downloaded this APP to do so without delay.

Estates Management Office  
Security Office