Уважаемые абитуриенты и их представители, коллеги!

В период проведения вступительных кампаний традиционно увеличивается количество попыток совершения мошеннических действий в отношении абитуриентов.

С целью осуществления мошеннических операций, а также вовлечения в граждан в экстремистскую и террористическую деятельность преступники создают фишинговые сайты организаций, в том числе вузов, банков, государственных учреждений.

В связи с этим Управление по комплексной безопасности напоминает правила, которые необходимо соблюдать, чтобы обезопасить себя и защитить свои средства от мошенников:

1. При возникновении сомнений в достоверности или подлинности поступившего сообщения (электронная почта, СМС, мессенджер) обязательно уточнять у отправителя по альтернативному каналу связи. Не пересылайте сообщение коллегам/ родственникам/ знакомым. Даже если отправитель Вам знаком, уточните у него факт отправки письма, возможно, его электронную почту или мессенджер взломали.

2. Проверьте, является ли сайт, на который вы хотите зайти, «безопасным»: в адресной строке Вашего браузера адрес сайта должен начинаться с «https://» и иметь пиктограмму закрытого замка. Зачастую на поддельных сайтах можно заметить орфографические ошибки или недочеты дизайна. При малейшем сомнении не вводите никаких данных на подозрительном сайте!

3. Обращайтесь по официальным каналам связи (телефон) лично.

4. Никому не сообщайте пароль от своего аккаунта в системе «Госуслуги».

5. Не вступайте в неофициальные группы (каналы) в мессенджерах.

- Не совершайте денежные операции по просьбе незнакомых людей.
- Никому не передавайте свою банковскую карту и доступ в свой онлайн-банк.
- Не сообщайте посторонним людям реквизиты своей карты, коды из СМС-сообщений или пуш-уведомлений.

6. С особой бдительностью проверяйте номер отправителя и ссылки в SMS сообщениях. Прерывайте разговор с абонентом, если он не может внятно объяснить цель своего звонка и (или) требует с Вас персональные данные.

7. Мошенники постоянно отслеживают появление новых возможностей и технологий, чтобы использовать их в своих целях. Например – видеосвязь: мошенники просят показать свой экран, для того, чтобы убедиться, что Вы делаете все правильно.

На самом деле они записывают Ваши данные, которые Вы в этот момент там вводите:

- пароль от почты, пароль от личного кабинета «Госуслуг»,
- пароль от личного кабинета Банка,
- голос с кодовым словом и др.

Если Вы подозреваете, что подверглись атаке мошенников, незамедлительно сообщите об этом в Управление по комплексной безопасности: 99-86-75.