ПРИЛОЖЕНИЕ

УТВЕРЖДЕНО
приказом и.о. ректора университета
от «12» 02 2025 г. № 65

ПАМЯТКА
о действиях при поступлении телефонных звонков или сообщений от имени якобы ваших руководителей и коллег

В последнее время резко участились случаи, когда Вы получаете звонок, сообщение, электронное письмо от имени руководителя организации, начальника вашего структурного подразделения или от коллег, которые сообщают вам важную для вас информацию, или просят совершить какие-либо действия.

Эти указания и просьбы могут направлять **МОШЕННИКИ** с помощью современных технических средств, при этом в Вашем телефоне будет отражаться ФИО руководителя (коллеги) и может содержаться его фото.

Например, некоторые **НАИБОЛЕЕ ЧАСТЫЕ СИТУАЦИИ**:

- получить подарок для ребенка от компании или разовую премию, заполнив анкету;
- «руководитель» информирует вас о проводящейся проверке в бухгалтерии, заведении на вас уголовного дела и т.д.; о том, что сейчас поступит звонок от «важного человека» и просит выполнить все, что тот скажет, вплоть до того, что потребуется взять кредит на свое имя «в интересах дела»;
- «руководитель» даёт указание оказать помощь/содействие в важном вопросе сотруднику полиции/ФСБ/налоговой службы «Петрову Ивану Петровичу», который вскоре Вам позвонит;
- звонок или сообщение от знакомого, который сообщает, что попал в тяжелую жизненную ситуацию и просит помочь – перевести деньги;
- поступление звонков якобы от сотрудников операторов связи сообщающих о том, что скоро заканчивается договор на услуги связи по вашей сим-карте. Мошенники уверенно заявляют, что это новые правила пользования мобильной связью, и теперь необходимо ежегодно продлевать ваш договор. И нужно для этого сообщить им код из смс, который сейчас придет на ваш телефон – тогда «сотрудники» подтвердят ваш номер на сайте Госуслуг;

- поступает звонок с угрозами отключения оборудования связи, видеонаблюдения и других технических средств;

- просят оценить работу курьера, оператора и т.д. и назвать код из СМС сообщения;

- иные подобные просьбы и указания, в том числе, вызывающие сомнения в их достоверности.

НЕ СПЕШИТЕ!

Порядок Ваших действий:

1. Внимательно **ПРОЧИТАЙТЕ** сообщение, **ПОДУМАЙТЕ**, почему звонят и присылают сообщение именно Вам, взаимодействовали ли Вы ранее таким образом.

2. **Обязательно ПЕРЕПРОВЕРЬТЕ информацию**! Перезвоните коллегам или руководителю, от которых пришло письмо или сообщение. Если обратный адрес не вызывает у вас подозрений, имейте в виду, что аккаунт может быть взломан. Будьте **особенно осторожны**, если получаете в мессенджере «срочное задание» или электронную ссылку.

3. **НЕ ПЕРЕХОДИТЕ ПО ССЫЛКАМ**, указанным в сообщении до тех пор, пока не убедитесь, в том, что вам их действительно прислали Ваши сотрудники или коллеги.

Цель мошенников одна – это получения кода из смс, чтобы завладеть вашими аккаунтами в банковском приложении или на портале госуслуг.

Затем – **ЗАВЛАДЕТЬ ВАШИМИ СРЕДСТВАМИ** или оформить на ваше имя займы в банке.

ЗАПОМНИТЕ – никогда не сообщайте незнакомым (а иногда и знакомым) людям по телефонам **никакие коды** подтверждений.

Обсуждайте все финансовые **вопросы лично**, а не в мессенджерах или по телефону.

БУДЬТЕ ПРЕДЕЛЬНО ВНИМАТЕЛЬНЫ И ОСТОРОЖНЫ!

При необходимости **обращаться** к заместителю начальника УКБиГО ВолгГТУ **Черкасову Алексею Викторовичу (тел. 24-80-32)**

Управление комплексной безопасности и гражданской обороны (УКБиГО) ВолгГТУ