СГХК
Корпоративное издание Степногорского горно-химического комбината
Полиметалл
№ 2 от 15 марта 2024 г.






Праздник женского очарования

Приход весны ознаменован самым прекрасным и нежным праздником - Международным женским днем. Современные женщины активно проявляют деловые и профессиональные качества. Они не только воспитывают детей, создают в домах тепло и уют, согревают родных и близких любовью, но еще и проявляют свой талант и способности на профессиональном поприще. Сегодня женщины являются активными участниками общественной и политической жизни республики.

Представительницы прекрасного пола в этот день в центре внимания – принимают поздравления от мужчин.

В преддверии 8 марта женщины комбината принимали поздравления. Руководство в лице генерального директора Жандоса Бекбаева, директора по производству Артема Важина, коммерческого директора Данияра Бейсембаева, главного инженера Андрея Черных пожелали женщинам-коллегам здоровья, семейного благополучия и успехов в труде. 16 женщинам были вручены благодарственные письма и ценные подарки. Также своих женщин-коллег поздравили руководство ТОО «Кызылту» и ТОО «СТЖ». Грамотой акима города была награждена Сыздыкова Гульнафиса Мусаевна, машиниста крана ремонтно-механического цеха.

Украсил мероприятие праздничный концерт.

Встречи с трудовым коллективом

5 марта прошли встречи руководства с трудовыми коллективами цехов, ставшие уже традиционными. Основной вопрос – повышение оплаты труда. Также были затронуты вопросы выполнения производственной программы, качества спецодежды, обуви, СИЗов и питания.

Приоритетным направлением является ремонт основного и вспомогательного оборудования для дальнейшего увеличения загрузки производства.

Установления "обратной связи" с работниками является действующим инструментом, который помогает своевременно принимать решения в звеньях руководства различного уровня.

НАШ СПОРТ

Завершены соревнования в рамках XXXI городской спартакиады

СГХК представил команды по всем видам спорта. Так, в январе состоялись соревнования по шашкам (2 место), шахматам (4 место), в феврале по тогызкумалаку (3 место), волейболу (3 место) и армрестлингу (1 место).

РАСПИСАНИЕ ЗАНЯТИЙ
в тренажерном зале и бассейне ДЮСШ «Батыр»
для работников СГХК, СТЖ, Кызылту

День недели	Тренажерный зал	Бассейн
Понедельник	19-20 ч.	20-21 ч.
Четверг	19-20 ч.	20-21 ч.

ВАКАНСИИ

- Специалист по надзору за строительством
- Мастер по ремонту электрооборудования
- Механик
- Энергетик
- Инженер-дозиметрист
- Инженер-конструктор
- Инженер по ремонту
- Инженер-технолог
- Мастер по КИПиА
- Фельдшер
- Экономист
- Грузчик-стропальщик
- Слесарь-ремонтник
- Электромонтер
- Токарь
- Электрогазосварщик
- Электрослесарь
- Транспортировщик

РЕЗЮМЕ: e-mail: Shevchenko.v@sghk.kz
Наличие резюме и квалификационных документов – обязательно.
Телефоны: 8(71645) 7-90-48 (коммутатор), вн. 715, 714, 746.

Полиметалл
Собственник: ТОО «Степногорский горно-химический комбинат»
Газета зарегистрирована в Министерстве культуры и информации Республики Казахстан
Свидетельство №8902-Г от 10.01.2008 г.
Редактор: Клавдия Швецова, shvetsova@sghk.kz
Газета отпечатана в типографии СГХК
Тираж: 60 экз.
Периодичность: 1 раз в месяц

БЕЗОПАСНОСТЬ

ОСТОРОЖНО МОШЕННИКИ!!!

Уважаемые жители г. Степногорск!

За 2023 г. от обманных способов интернет-мошенников жертвами среди населения Степногорского региона стало - 73 жителя, из них:

45 женщин: в возрасте 35-55 лет — 19 жен., 55-70 лет — 26 жен.;

28 мужчин: в возрасте 35-55 лет — 14 муж., 55-70 лет — 14 муж.

Общий ущерб составил около 150 000 000 тенге.

Одним из видов интернет-мошенничества является следующий способ:

вам звонят и представляются сотрудниками операторами любой связи и задают вам вопрос о том, собираетесь ли вы дальше пользоваться своим абонентским номером? Вы говорите: «да», после чего, вас уведомляют о том, что сейчас на ваш телефон поступит СМС сообщение якобы для того, чтобы вы далее смогли пользоваться своим номером телефона. Заполучив код подтверждения, мошенники оформляют на вас кредит в банке, так как СМС поступило не от оператора связи, а от вашего Банка.

В связи с участившимися случаями интернет-мошенничествами в приложении Kaspi.kz предупреждаем: при какой-либо покупке товара в Kaspi.kz мошенники путем обмана под разными предлогами, сообщают клиенту о необходимости отмены покупки, в последующем переводят клиента на сделку и оплату товара в мессенджере WatsApp, где скидывают ссылку на оплату товара. Уважаемые жители убедительная просьба, если вы столкнулись с подобным случаем просим не производить оплату по поступившей вам ссылке, НЕ ВЕРЬТЕ — ЭТО МОШЕННИКИ. Вся оплата за товары производится строго в самом приложении Kaspi.kz, просим проверять данные поставщика и саму оплату.

Если вам поступил звонок с неизвестного номера и представился:

- сотрудником банка;
- сотрудником полиции по выявлению мошенников;
- сотрудником оператора любой Казахстанской связи;
- сотрудником полиции и сообщил, что ваш близкий родственник попал в беду;
- если нашли объявление с рекламой, о получении: дополнительных выплат от государства, дивидендов от государственных программ, выплат путем внесения инвестиции в платформу «КАЗМУНАЙГАЗ», приобретении криптовалют и биткоинов,

НЕ ВЕРЬТЕ — ЭТО МОШЕННИКИ!!

Новые схемы мошенников заключается в том, что Вам могут позвонить с неизвестного номера на мессенджер WatsApp по видео звонку, представится сотрудником силовых структур (КНБ, МВД). Выходить на видеосвязь не рекомендуется. Мошенники могут записать ваше изображение и в дальнейшем использовать его для кражи денежных средств с помощью программ удаленного доступа, легенды злоумышленники используют разные, но суть их одна. Уважаемые граждане будьте бдительны и не поддавайтесь на уловки мошенников.

Мошенники неправомерно используют программы удаленного доступа, чтобы подключиться к вашему компьютеру, мобильному устройству и украсть ваши, коды доступа и даже деньги. Если же вы скачали программу удаленного доступа по просьбе мошенников и чувствуете опасность, прервите телефонный звонок, просто положив трубку. Прервите любую сессию удаленного доступа, просто выключив устройство.

Уважаемые жители города Степногорск!!! Убедительная просьба — БУДЬТЕ БДИТЕЛЬНЫ. Не поддавайтесь на уловки ИНТЕРНЕТ-МОШЕННИКОВ.

Базовые понятия, о которых надо знать каждому

• **Социальная инженерия** – обман человека с целью побуждения к действиям, выгодным злоумышленнику. Например, вам звонят и говорят: «Я из службы поддержки банка. Вам нужно сообщить мне код из SMS, который вам пришел». Это был обман и побуждение к действию, выгодному злоумышленнику. Отдельные атаки социальной инженерии могут осуществляться без использования технических средств. Метод основан на использовании человеческих слабостей и является очень эффективным.

• **Фишинг** (англ. phishing от fishing – рыбная ловля, выуживание) – процесс выманивания конфиденциальной информации через электронные коммуникации. Например, вы вводите пароль от аккаунта в социальной сети на поддельном сайте и нажимаете «Войти» – этот процесс называется фишингом.

• **Фишинговая ссылка** – адрес страницы, на которой злоумышленник крадет конфиденциальную информацию, оставляемую жертвой. Например, ссылка, после перехода по которой у вас просят ввести пароль от почты на поддельном сайте. Фишинговые ссылки могут поступать через все каналы: социальные сети, личный и рабочий e-mail, мессенджеры, SMS, а также чаты на сайтах знакомств и подобных ресурсах.

Внимание! Основные способы защиты от социальной инженерии — это информированность и недоверчивость.

• **Универсальное правило № 1:** Перепроверяйте любые просьбы связанные с финансами, с раскрытием информации (в том числе личной и финансовой), с переходами по ссылкам, связываясь с просящим по каналу связи, отличному от того, по которому пришла просьба. Перезванивайте «коллегам» и «родственникам», которые просят перевести деньги, «знакомым» которые просят проголосовать за ребенка и удостоверяйтесь, что сообщение получено от них.

• **Универсальное правило № 2:** Лучше не открывать ссылки от незнакомцев.

• **Универсальное правило № 3:** Даже ваших знакомых могут взломать. Если они вам прислали ссылку без объяснения или с подозрительным объяснением (например, как продолжение разговора, которого не было), стоит обратиться к ним напрямую, позвонив и уточнив информацию.

• **Универсальное правило № 4:** Ни в коем случае не устанавливайте программы удаленного управления (TeamViewer, AnyDesk и аналогичные) по просьбе посторонних лиц. С помощью данных программ возможно получение полного контроля над вашим устройством.

• **Универсальное правило № 5:** Никому никогда не сообщайте СМС-коды и пароли.

• **Универсальное правило № 6:** Если после перехода по подозрительной ссылке у вас запрашивают конфиденциальную или личную информацию, предлагают скачать файл (особенно архив) – уходите с сайта.

• **Универсальное правило № 7:** Всегда пользуйтесь современным антивирусом, который может распознать фишинговую ссылку еще «на подлете».

• **Универсальное правило № 8:** Проверяйте ссылку не только перед переходом по ней, но и когда вы уже перешли на сайт. Сайт, на который вы попали, может отличаться от того, что было написано в ссылке.