Министерство социальной политики
Свердловской области

Профилактика хищений денежных средств граждан с использованием информационно-телекоммуникационных технологий (ИТТ)

Защита государственного гражданского служащего
в цифровую эпоху

Цифровые угрозы - невидимый враг

Рост IT-преступлений

Число преступлений с использованием информационно-телекоммуникационных технологий в 2024 году продолжает стремительно расти. Мошенники совершенствуют методы и атакуют всё более изощрённо.

Государственный служащий - приоритетная цель

Доступ к конфиденциальной информации делает государственного служащего мишенью для кибершпионов, хактивистов и кибермошенников.

Основные векторы атак

Фишинг, вредоносное ПО и целевые атаки (APT)* - главные инструменты злоумышленников.

*(Advanced Persistent Threat, «продвинутая устойчивая угроза»)

Нормативная база

Мошенничество

Статья 159 Уголовного кодекса Российской Федерации
Особенности квалификации часть 3 и часть 4 (крупный и особо крупный размер)

Неправомерный доступ к компьютерной информации и создание вредоносных программ

Статья 272, 273 Уголовного кодекса Российской Федерации

Нарушение законодательства о персональных данных, как фактор способствующий хищению

Статья 13.11 Кодекса Российской Федерации об административных правонарушениях

Искусство обмана — как мошенники заманивают жертв

Фишинг

Поддельные письма от руководства, IT-отдела или партнёров. Признаки: срочность, давление, подозрительные ссылки, вложения с расширениями .zip, .js, .exe.

Безопасный счет

Звонки от имени правоохранительных органов или Банка России: Легенда о «безопасном счете», попытке оформления кредита третьими лицами.

Спам

Массовые рассылки, часто содержащие вирусы или ведущие на вредоносные сайты.

Кликбейт

Захватывающие заголовки, обещающие выигрыши, призы или лёгкие деньги. Цель - заставить кликнуть на вредоносную ссылку.

Ваша бдительность - первая линия обороны.

Осведомлённость и соблюдение правил цифровой гигиены - главные инструменты защиты от киберугроз.

«Золотые правила» для разъяснения гражданам:

Сотрудник банка (или госоргана) никогда не запрашивает пароли из СМС и данные карт по телефону.

Правило «положения трубки» - необходимо самостоятельно перезвонить в банк по номеру, указанному на обороте карты.

Понятие «период охлаждения» для кредитов - как им пользоваться.

Цифровая гигиена - ваш щит в онлайн-мире

Правила Минцифры для государственных гражданских служащих:

Не открывайте подозрительные ссылки и вложения

Даже если письмо кажется официальным - проверяйте источник.

Используйте сложные пароли

Не менее 12 символов: буквы, цифры, спецсимволы. Меняйте каждый месяц.

Не используйте одинаковые пароли

Каждая учётная запись - уникальный пароль.

Не сообщайте логины и коды из SMS

Настоящие сотрудники никогда не запрашивают эти данные.

Осторожно с финансовыми письмами

Письма с угрозами или финансовыми темами - повод для повышенной настороженности.

Управление учётными записями — крепость ваших данных

Надёжные пароли

Не менее 12 символов: заглавные и строчные буквы, цифры, спецсимволы. Без личной информации и простых последовательностей.

Менеджеры паролей

Используйте KeePass или Bitwarden для создания и хранения уникальных паролей.

Двухфакторная аутентификация (2FA)

Второй рубеж обороны - даже если пароль украден, злоумышленник не получит доступ.

Двухфакторная аутентификация: ваш второй барьер

Что-то, что вы знаете	Что-то, что у вас есть
Пароль	Телефон или токен

Результат

Максимальная защита

Распознавание угроз - будьте на шаг впереди

Проверка отправителя

Знаком ли вам отправитель? Совпадает ли адрес с официальным доменом организации?

Анализ URL-ссылок

Убедитесь, что адрес сайта официальный. Подозрительные домены — признак фишинга.

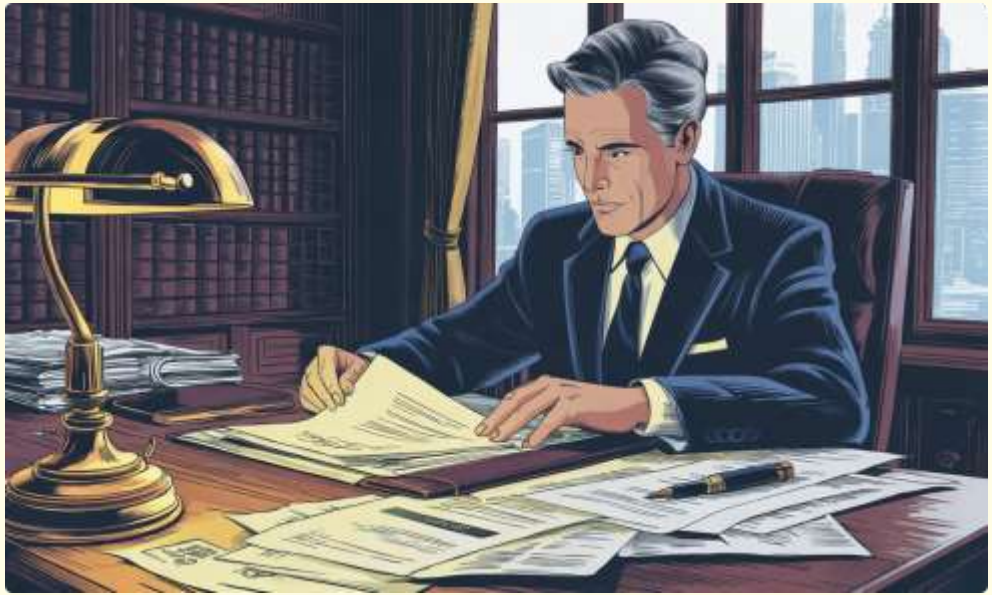
Макросы в документах

Отключите исполнение макросов, если вы ими не пользуетесь. Они могут содержать вредоносный код.

Подозрительные сообщения

Если разговор кажется странным — завершите его и перезвоните по официальному номеру.

Ответственность и профилактика — ваша роль в общей безопасности



Личная ответственность

Кибергигиена - не рекомендация, а ваша обязанность как государственного служащего.

Последствия халатности

Утечка данных граждан, срыв госпрограмм, финансовый ущерб и подрыв национальной безопасности.

Постоянное обучение

Следите за новыми видами мошенничества и методами защиты - угрозы эволюционируют.

Безопасность в ваших руках

Ваша бдительность и соблюдение правил цифровой гигиены - ключ к предотвращению хищений денежных средств граждан и обеспечению информационной безопасности государства.

Будьте бдительны

Проверяйте каждый источник

Соблюдайте правила

Кибергигиена - ваша обязанность

Создаём безопасность вместе

Присоединяйтесь к защите цифрового пространства