



ҚАРЖЫЛЫҚ САУАТТЫЛЫҚ

20 минуттық қорғаныс курсы

Интернет қолданушыларына арналған

2025 жыл

МАЗМҰНЫ

01

Қаржылық негіз

5 мин

02

Онлайн қауіпсіздік

5–7 мин

03

Алаяқтықты тану

5–8 мин

04

Курс нәтижесі



Бюджет жоспарлау

Табыс пен шығысты бақылаңыз



Цифрлық қауіпсіздік

Парольдер мен 2FA



Фишинг пен алаяқтық

Қауіпті схемаларды тану



Нәтиже

Білім мен дағды

Неге бұл курс маңызды?

₸2.1 трлн

Қазақстандықтар жоғалтқан қаражат
(алаяқтық, 2023)

68%

Қолданушылар онлайн қаржылық
қауіпке ұшырайды

3 мин

Орташа алаяқтардың шабуыл жасау
уақыты

КУРС МАҚСАТЫ

Қатысушыларға қаржыны дұрыс басқарудың негізгі қағидаларын және интернеттегі қаржылық алаяқтықтан қорғанудың қарапайым әдістерін үйрету.



Табыс пен шығысты ажырату

1

Табыс — кіріс ақша ағыны

Жалақы, бизнес, пассивті кіріс, жәрдемақы — барлық кіретін қаражат.

2

Шығыс — шығатын ақша ағыны

Тұрмыстық, тамақ, несие, ойын-сауық — барлық кететін қаражат.

3

Алтын ереже: Табыс > Шығыс

Айлық шығысыңыз табысыңыздан аспасын. Айырмасы — сіздің болашағыңыз.



50/30/20 Бюджет ережесі

50%

ҚАЖЕТТІЛІКТЕР

- ✓ Жалдау / баспана
- ✓ Тамақ
- ✓ Коммуналдық
- ✓ Көлік

30%

ҚАЛАУЛАР

- ✓ Ойын-сауық
- ✓ Сапарлар
- ✓ Кино, кафе
- ✓ Жаңа заттар

20%

ЖИНАҚ & БОРЫШ

- ✓ Жинақ шот
- ✓ Инвестиция
- ✓ Несие өтеу
- ✓ Шұғыл қор



Жинақ жасаудың маңызы

1

Шұғыл қор — 3–6 айлық шығыс

Кенеттен жұмыссыз қалу, ауру немесе апат болғанда сізді қорғайды.

2

Алдымен өзіңізге төлеңіз

Жалақы алған сәтте алдымен жинаққа салыңыз, содан соң жұмсаңыз.

3

Ең болмаса табысыңыздың 10% жинаңыз

Аз болса да тұрақты жинақ үлкен нәтиже береді. Шағын қадам — үлкен мақсат.



Қауіпсіз пароль жасау

1

Кем дегенде 12 символ, аралас таңба қолданыңыз

Бас/кіші әріп, сан, арнайы белгі (@#\$%^&*) — бәрін біріктіріңіз.

2

Әр сайтқа жеке пароль жасаңыз

Бір пароль ашылса — барлық аккаунттарыңыз қауіпте. Менеджер (Bitwarden, 1Password) қолданыңыз.

3

Жеке деректерді пайдаланбаңыз

Туған күн, аты-жөн, телефон — хакерлер бірінші осыларды тексереді.

Екі факторлы қорғаныс (2FA)

2FA дегеніміз не?

Кіру кезінде пароль + қосымша растау кодын сұрайтын қауіпсіздік жүйесі. Пароль ұрланса да, хакер кіре алмайды.

ЕСКЕРТУ

2FA кодын ешкімге жіберме!
Банк қызметкерлері де сұрамайды.

1

Банк/сайтта 2FA қосыңыз

Параметрлер → Қауіпсіздік → 2FA

2

Google Authenticator немесе SMS

Кодты телефоныңызға алыңыз

3

Кіру кезінде кодты енгізіңіз

30 секунд ішінде жаңарады

Банк картасын қорғау ережелері

1

Картаңыздың деректерін ешкімге бермеңіз

CVV кодын, PIN-кодты, OTP-кодты банк өзі де сұрамайды. Сұраса — алаяқ!

2

Сенімді сайттарда ғана төлем жасаңыз


URL-де 'https://' және құлып белгісі болуы тиіс. HTTP сайтта карта мәліметін енгізбеңіз.

3

SMS хабарландыруды қосыңыз

Барлық транзакцияны бақылаңыз. Күмәнді операция болса — картаны дереу блоклаңыз.

Фишинг дегеніміз не?

 Фишинг — алаяқтардың сізді жалған сайтқа немесе хабарламаға алдап, жеке деректеріңізді немесе ақшаңызды ұрлауға тырысуы.



Жалған сілтеме (URL)

Мыс: kaspi-bank.kz.fake.com — шынайы емес!



Шұғыл мазмұнды хат

"Аккаунтыңыз бұғатталды! Дереку кіріңіз!" — дүрбелең туғызады.



Тым тиімді ұсыныс

"Сіз 1 000 000 ұтып алдыңыз!" — шындық емес.



Деректерді сұрау

Пароль, карта нөмірі, SMS-код сұраса — тоқтаңыз.



Нақты оқиға: Google Docs Phishing Attack

2017

Шабуыл

1 млн+ Gmail қолданушысы жалған «Google Docs» сілтемесі бар хат алды.

Хат

Мазмұны

"Сіздің досыңыз Google Docs файлын ортақтасты. Ашу үшін басыңыз."

Шерту

Нәтиже

Шерткен соң — шынайы Google беті шықты, бірақ зиянды қосымша рұқсат сұрады.

Ақыр

Зардап

Қолданушының барлық контактарына осы хат автоматты жіберілді. 1 сағатта таралды.

Күмәнді қоңыраулар мен «инвестиция» ұсыныстары

1

«Сіздің шотыңыз бұғатталды» — классикалық алдау

Банк телефон арқылы ешқашан пароль, CVV немесе SMS-кодты сұрамайды. Қоңырауды үзіп, банктің ресми нөміріне өзіңіз қоңырау шалыңыз.

2

«Тез байы!» инвестиция схемалары

«Айына 50% пайда» — мүмкін емес. Пирамида схемалары заңды инвестиция деп өздерін таныстырады. Ресми лицензияны тексеріңіз.

3

Шұғыл қысым — алаяқтың белгісі

«Қазір шешім қабылдасаңыз, ұтылып қаласыз!» — бұл манипуляция. Асықпаңыз, жақындарыңызбен кеңесіңіз.

«КиберҚалқан» жүйесін тиімді қолдану



Алаяқтық сайттарды тексеру

Күмәнді сілтемені КиберҚалқанға жіберіп, дереу тексеруден өткізіңіз.



Оперативті хабарландыру

Жаңа алаяқтық схемалар туралы жедел ескерту алыңыз.



Шағым беру мүмкіндігі

Алаяқтықпен кездессеңіз — жүйе арқылы тікелей хабарлаңыз.



Білім базасы

Қауіпсіздік бойынша нұсқаулықтар мен жаңартылған деректер.

КУРС НӘТИЖЕСІ

Сіз не үйрендіңіз?



Қаржысын жоспарлаудың 50/30/20 тәсілін біледі



Күшті пароль жасап, 2FA қосу дағдысын меңгерді



Күмәнді сілтеме мен хабарламаны ажырата алады



Алаяқтық схемалардың негізгі белгілерін таниды



«КиберҚалқан» жүйесін тиімді қолдана алады



Ақпарат көздері

1 Қазақстан Республикасы Ұлттық Банкі — Қаржылық сауаттылық порталы: fingramota.kz

2 Қазақстан Республикасы АҚШ — «КиберҚалқан» ұлттық киберқауіпсіздік жүйесі

3 Google Security Blog — The Google Docs Phishing Attack (2017): security.googleblog.com

4 OECD — Financial Literacy and Inclusion: 2023 Annual Report

5 Kaspersky Lab — Фишинг шабуылдарының 2023 жылғы статистикасы: securelist.com

6 National Cybersecurity Alliance — nca.org: Онлайн қауіпсіздік бойынша нұсқаулықтар