# Сигурни ли са семейните Ви финанси в дигиталния свят?

*В училище Вашето дете започна работа по темата за финансовата киберсигурност. Може би се питате: „Защо сега?“ и „Не е ли твърде малко за тези неща?“. Истината е, че днешните деца разполагат с достъп до банкови карти, онлайн игри и социални мрежи много по-рано от всяко предишно поколение. Те са уверени потребители, но често им липсва житейски опит, за да разпознаят кога някой се опитва да ги манипулира.*

## Защо е важна Вашата роля?

*Ние в училище полагаме основите, но навиците се изграждат у дома. Измамниците не атакуват компютрите – те атакуват хората. Те разчитат на нашето бързане, на родителската ни тревога или на детското любопитство. Тази брошура не е списък със забрани. Тя е инструмент, който ще Ви помогне да превърнете темата за сигурността в нормален разговор около вечерята.*

## Какво ще научите от тези страници:

- Как да разпознавате петте най-разпространени схеми за кражба на данни.
- Кои са психологическите „кукички“, на които се хващаме най-лесно.
- Как да проведете разговор с детето си, без да го плашите, а като го овластявате.
- Как да тествате знанията си заедно чрез интерактивна симулация.

VISA

преподаваме.bg

# Петте капана

## Фишинг (Phishing) – „Въдицата“ в пощата

- **Какво е:** *Имейл, който имитира позната институция (банка, Еконт, Netflix).*
- **Пример:** Получавате писмо: *„Вашият абонамент изтича. Актуализирайте данните за плащане тук, за да не загубите достъп.“ Линкът Ви води към сайт, който изглежда досущ като истинския, но е създаден, за да запише номера на картата Ви.*

## Смишинг (Smishing) – Опасност в джоба

- **Какво е:** *Фишинг, но чрез SMS. По-опасен е, защото хората се доверяват повече на съобщенията в телефона си.*
- **Пример:** *„Имате пратка с номер 12345. За да я получите, платете такса от 1.45 лв. на този адрес.“ Детето Ви може да очаква поръчка от онлайн магазин и лесно да кликне.*

## Спуфинг (Spoofing) – Маскираният измамник

- **Какво е:** *Техническа измама, при която имейл адресът или телефонният номер на подателя изглеждат напълно легитимни.*
- **Пример:** *Звъни Ви телефонът и на екрана пише името на Вашата банка. „Служителят“ Ви казва, че има съмнителна трансакция и трябва спешно да потвърдите паролата си, за да спрете тегленето.*

## Скуатинг (Typosquatting) – Капанът на грешката

- **Какво е:** *Регистрация на сайтове с имена, в които има малка правописна грешка.*
- **Пример:** *Детето иска да влезе в roblox.com, но изписва robl0x.com (с нула вместо „о“). Фалшивият сайт предлага „безплатни бонуси“ срещу въвеждане на данните за вход в профила.*

## Скиминг (Skimming) – Физическата кражба

- **Какво е:** *Устройства, монтирани върху банкомати или терминали, които копират магнитната лента на картата.*
- **Пример:** *Плащате на автомат на бензиностанция или паркинг. Четецът на карти изглежда леко разхлабен или по-дебел от обикновено. Скрита камера или фалшива клавиатура записва Вашия ПИН код.*

VISA

преподаваме.bg

# Психология и разговор с детето

## Защо умни хора стават жертва на измами? Защото измамниците не използват код, а емоции. Те „хакват“ човешкото внимание чрез:

- **Спешност:** „Имате само 10 минути, преди сметката Ви да бъде блокирана!“
- **Страх:** „Вашият акаунт е използван за незаконни цели. Потвърдете самоличността си.“
- **Алчност:** „Вие сте 1 000 000-ият посетител! Спечелихте награда!“
- **Авторитет:** Използване на лога на държавни институции, МВР или големи компании.

## Как да говорите за това с Вашето дете?

## Вместо лекция тип „Не прави това“, опитайте партньорски подход:

- **Споделете собствения си опит:** Разкажете за съмнителен имейл, който сте получили. Попитайте детето: *„Как мислиш, по какво познах, че това е измама?“*.
- **Уговорете „Семейно правило за пауза“:** Научете детето, че ако някога види съобщение, което го кара да се чувства притеснено или превъзбудено, трябва първо да дойде при Вас, преди да кликне.
- **Проверете настройките заедно:** Прегледайте паролите и двуфакторната автентикация (2FA) на неговите профили в игрите и социалните мрежи. Обяснете му, че това са ключовете за неговата дигитална стая.

VISA

преподаваме.bg

# Практически протокол и симулация

Когато получите съобщение, което изисква действие от Ваша страна, приложете този 3-степенен протокол за безопасност:

- **СПРЕТЕ:** Не предприемайте действие веднага. Измамниците печелят, когато бързате.
- **ПРОВЕРЕТЕ:** Погледнете внимателно имейл адреса на подателя. Има ли правописни грешки? Линковете водят ли към официалния сайт? (Задръжте мишката върху линка, без да кликате, за да видите реалния адрес).
- **ПОТВЪРДЕТЕ:** Ако съобщението твърди, че е от банката Ви, затворете го и влезте в официалното им приложение или им се обадете по телефона. Никога не използвайте предоставения в съобщението линк.

**Упражнение за цялото семейство:** Каним Ви да се включите в мисията, която учениците изпълниха в час. Симулацията **Cyberguard** ще Ви постави в 8 реални ситуации – от съмнителни SMS-и до манипулирани банкомати.

- **Как да започнете:** Сканирайте QR кода или посетете prepodavame.bg/finansova-kibersigurnost
- **Цел:** Опитайте се да преминете през всички нива без нито една грешка. Ако сгрешите – прочетете внимателно обратната връзка. Тя ще Ви каже точно на какво да обръщате внимание следващия път.

**За prepodavame.bg:** Ние сме платформа, която подкрепя българските учители с практически ресурси за съвременно преподаване. Този материал е част от стремежа ни да свържем училището с реалния живот. Вашето мнение е важно за нас – споделете опита си от използването на този наръчник на нашия сайт.

VISA

преподаваме.bg