

Как да плащам безопасно онлайн?

Научи начините, по които можеш да станеш жертва на интернет измама.



ФИШИНГ (Phishing)

Фалшиви имейли или съобщения, които изглеждат истински и искат лични данни.

Ели получава имейл от куриерска фирма, в който пише, че трябва да плати малка такса, за да получи пратката си. Имейлът я препраща към сайт, който иска данните на картата ѝ. Тя ги въвежда, мислейки, че плаща таксата, но по-късно открива неотризирирани транзакции.

Стефан получава имейл, който уж е от популярна стрийминг платформа. Имейлът твърди, че абонаментът му ще бъде прекратен, ако не актуализира данните си за плащане. В паниката си той кликва върху линка и въвежда данните на картата си, които веднага се използват за неразрешени покупки.



Как да се предпазя от фишинг?

Проверявай адреса на изпращача и никога не споделяй пароли.

СМИШИНГ (Smishing)

Като фишинг, но чрез SMS съобщения или обаждания, понякога с помощта на AI.

Петя получава SMS, който я уведомява, че е спечелила чисто нов телефон. За да го получи, тя трябва да кликне на линк и да въведе личните си данни, които после са използвани за злоупотреба.

Мартин получава обаждане от човек, който твърди, че е представител на мобилния му оператор. Той обяснява, че трябва да потвърди кода, който току-що му е изпратен в SMS. В действителност, с този код измамникът активира достъп до онлайн профила му.



Как да се предпазя от смишинг?

Игнорирай съобщения от непознати номера и подозрителни обаждания.

СКИМИНГ (Skimming)

Кражба на данни за карти или акаунти чрез бисквитки или фалшиви сайтове.

Мария решава да купи подарък онлайн и попада на сайт, който изглежда точно като ozone.bg. Тя въвежда данните си, но по-късно разбира, че парите ѝ са изчезнали, защото сайтът е бил фалшив.

Кристина поръчва доставка на храна през ново приложение, което има минимални изисквания за сигурност. Скиминг софтуер, скрит в платформата, записва информацията за картата ѝ, която по-късно се използва за измами.



Как да се предпазя от скиминг?

Пазарувай само от сайтове, започващи с "HTTPS" (S = Secure/Безопасен) и иконка със заключен катинар.

СКУАТИНГ (Squatting)

Иво последва линк, получен в имейл от любимия му сайт „favoriteshop.bg“. Прави поръчка и въвежда данните на картата си. Чак след това вижда, че адресът на сайта е „favoritesshop.bg“, но вече е бил измамен.

Сайтове с фалшиви адреси и дизайн, които имитират истински.

Калина иска да си купи обувки от сайт, който прилича на официалния сайт на любимата ѝ марка. Адресът изглежда почти идентичен, но има добавен знак „-“. Тя поръчва и плаща обувките, но те никога не пристигат.



Как да се предпазя от скуатинг?

Проверявай уеб адресите за грешки като „gougle.com“, „g00gle.com“, „google.net“ или „gogle.com“ вместо „google.com“.

СПУУФИНГ (Spoofing)

Стоян получава имейл, който изглежда изпратен от IT отдела на работата му. В писмото се иска да потвърди паролата си за достъп до корпоративната мрежа. След като я въвежда, достъпът до профила му е компрометиран.

Фалшиви линкове, имейли или номера, които изглеждат истински.

Антон получава имейл от банка ДСК, в който пише, че трябва спешно да въведе паролата си, за да се избегне блокиране на сметката му. Логото и стилът на текста са идентични с тези на истинската банка. Линкът също изглежда истински: „account.dskbank.bg“, но Антон не забелязва, че всъщност води до друг сайт, който краде данните му.



Как да се предпазя от спууфинг?

Не кликай на линкове без да провериш адреса.

Никой доверен няма да ти поиска:

- Пароли
- Платежни данни (номер на карта)
- Адрес
- Имена, ЕГН

Банките, куриерите и онлайн търговците вече имат достъп до тези данни в потребителския ти профил.

Преди да кликнеш върху линк:

- Очакваш ли такъв имейл/SMS?
- Изпращачът истински ли е?
- Адресът/телефонът на изпращача изглежда ли надежден?
- Проверявай езика, логото и сайта за грешки.



Какво се случва, когато плащаме с карта?

Когато някой плати с карта, парите минават през банката на купувача, платежната система (като Visa) и банката на продавача. Всичко това става за секунди!

Парите в картата не са физически като банкнотите – те са числа в системата. Картите са удобни, защото не трябва да носиш пари в брой, а и плащанията са по-бързи и по-сигурни (ако знаеш как да пазиш).

