



**Инструментите,  
използващи изкуствен  
интелект, дават нов  
тласък на хакерите.**

**Подготвени ли сте?**



## До сега...

Умелите измамни атаки изискваха много време и усилия и можеха да се постигнат само от наистина обиграни хакери.

В резултат на това **повечето опити за фишинг бяха на аматорско ниво** (напр. с правописни грешки, съмнителен дизайн, развален език и т.н.) и фалшивите съобщения се разпознаваха с лекота.







## Днес...

С помощта на инструментите, работещи с изкуствен интелект, хакерите могат бързо и лесно да създават имейли и съдържание на истински професионално ниво.

Вследствие на това **до пощенските ни кутии вече достигат все по-изкусно създадени атаки.** Тези умели измамни атаки по-трудно се разпознават като заплаха, което повишава риска да се хванем на въдицата.

# Как да разпознаем опитите за фишинг в днешно време?

- При имейлите се уверете, че **адресът на подателя** се показва точно както очаквате. Хакерите не могат да фалшифицират този детайл.
- Задържайте мишката над **линковете**, преди да ги отворите, за да се уверите, че изглеждат достоверни. Хакерите могат да имитират дизайна на известни компании, но не и да използват оригиналните им домейни.



## Кое вече **не се счита** за надежден признак за автентичност?

- Професионален дизайн
- Добре написан текст
- Гласов запис на човек, когото познавате
- Висококачествени видеа



## **Запомнете: Нашата безопасност е в собствените ни ръце.**

Създайте си навика да  
проверявате щателно всеки  
имейл, преди да отворите  
каквито и да е линкове, и никога  
не проверявайте имейлите си,  
когато сте разконцентрирани.

