

Как да разпознаем фишинг имейл

Петте признака, които издават измамното съобщение — и правилото на 60-те секунди.

ПЕТТЕ ПРИЗНАКА

1

Истинският адрес не съвпада

Гледайте пълния адрес на подателя, не показаното име: paypal.com не е paypal.com.

2

Изкуствена спешност

„До 24 часа“, „незабавно действие“: натискът сам по себе си е алармен сигнал.

3

Линкът не води където показва

Задръжете курсора, без да кликате: истинската дестинация се показва долу. Дълго натискане на телефона.

4

Неочакван прикачен файл

Основният път на рансъмуера. Потвърдете през друг канал, преди да отворите — и правете резервни копия.

5

Искане на чувствителна информация

Никоя легитимна организация не иска пароли или номера на карти по имейл.

Правилото на 60-те секунди

1. Затворете имейла — без отговор, без клик.
2. Отворете нов раздел и влезте сами в официалния сайт.
3. Проверете дали проблемът наистина съществува. Почти винаги: не.

Спешността е тяхното оръжие. Времето е вашето.

Сигнал и реакция

Сигнали за измамни съобщения: cybercrime.bg (ГДБОП).

Отворен по грешка прикачен файл: антивирусно сканиране + сменете паролите си.

Официална и безплатна помощ: cybercrime.bg (ГДБОП)