KORZYŚCI SYMULOWANYCH TESTÓW PHISHINGOWYCH

1

PODNIESIENIE ŚWIADOMOŚCI PRACOWNIKÓW

Testy uświadamiają pracownikom realne zagrożenie phishingiem i uczą ich rozpoznawać podejrzane wiadomości. Nawet jeśli "dadzą się złapać", staje się to cenną lekcją na przyszłość.

2

IDENTYFIKACJA SŁABYCH PUNKTÓW

Pozwalają zidentyfikować, którzy pracownicy lub działy są najbardziej podatni na ataki phishingowe. Umożliwia to skierowanie dodatkowych szkoleń i zasobów tam, gdzie są najbardziej potrzebne.

3

MIERZENIE EFEKTYWNOŚCI SZKOLEŃ

Regularne symulacje pozwalają ocenić, czy dotychczasowe szkolenia z zakresu cyberbezpieczeństwa przynoszą oczekiwane rezultaty i czy pracownicy stosują zdobytą wiedzę w praktyce.

4

REDUKCJA RYZYKA RZECZYWISTYCH ATAKÓW

Pracownicy, którzy regularnie uczestniczą w symulacjach, stają się bardziej ostrożni i mniej podatni na rzeczywiste ataki phishingowe.

5

SPEŁNIENIE WYMOGÓW REGULACYJNYCH

W niektórych sektorach regularne testowanie i szkolenie pracowników w zakresie cyberbezpieczeństwa może być wymogiem prawnym lub standardem branżowym.

SYSBIT.IT