BEZPIECZEŃSTWO W CZASACH KRYZYSU

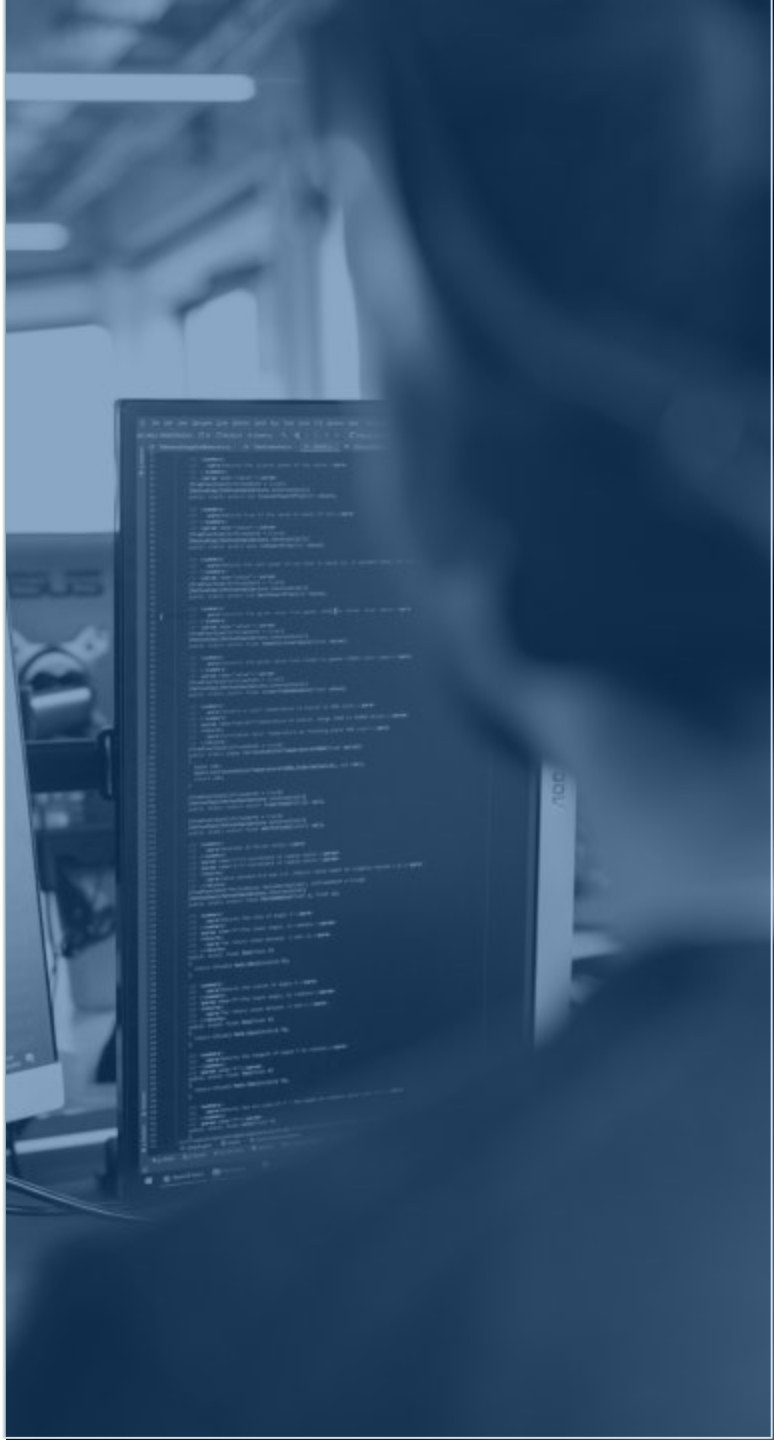
March, 2022

Powered by

Dlaczego ma to znaczenie

Nasila się aktywność cybernetyczna wokół konfliktu na linii Rosja–Ukraina i choć nie jesteśmy w niego bezpośrednio zaangażowani, dotyczy on nas wszystkich.

Każdy kryzys światowy ma wymiar cybernetyczny, a gwałtowny wzrost liczby złośliwych wiadomości phishingowych świadczy o tym, że ten kryzys nie jest inny.



Co się dzieje

1 Obie strony przeprowadzają wzajemne ataki cybernetyczne, obejmujące złośliwe oprogramowanie usuwające dane oraz wyłączanie stron internetowych z sieci w celu uniemożliwienia korzystania z nich.

2 Ataki te nie zawsze udaje się opanować i często infekują one urządzenia i strony internetowe, które nie są zaangażowane w konflikt. Dotyczy to również urządzeń firmowych i osobistych.

3 Twoje osobiste konta w mediach społecznościowych są również narażone na ryzyko włamania się do nich w celu rozpowszechniania fałszywych informacji lub złośliwego oprogramowania.

Co możesz zrobić, aby chronić swoją sieć domową

Zainstaluj aktualizacje systemu operacyjnego i zabezpieczeń. Jeśli są one dostępne, na komputerze lub telefonie powinno pojawić się powiadomienie.

Dodaj drugi czynnik uwierzytelniania do swoich kont w mediach społecznościowych (Facebook, Linkedin, Twitter itp.) oraz kont poczty elektronicznej. Jeśli to możliwe, dodaj także zapasowy adres e-mail.

Powiadamiaj swoich przyjaciół i rodzinę o tym, co się dzieje, i zachęć ich do robienia tego samego.

Co możesz zrobić, aby chronić naszą sieć

Damy o bezpieczeństwo sieci wewnętrznej, więc nie musisz podejmować żadnych technicznych kroków.

W tym czasie może dojść do większej liczby ataków phishingowych. Uważaj na e-maile z prośbą o pomoc w sprawach technicznych lub finansowych.

Zawsze sprawdzaj adres e-mail nadawcy — pamiętaj, że jest to najważniejszy krok w wykrywaniu phishingu.