СИГУРНОСТ ПО ВРЕМЕ НА КРИЗА

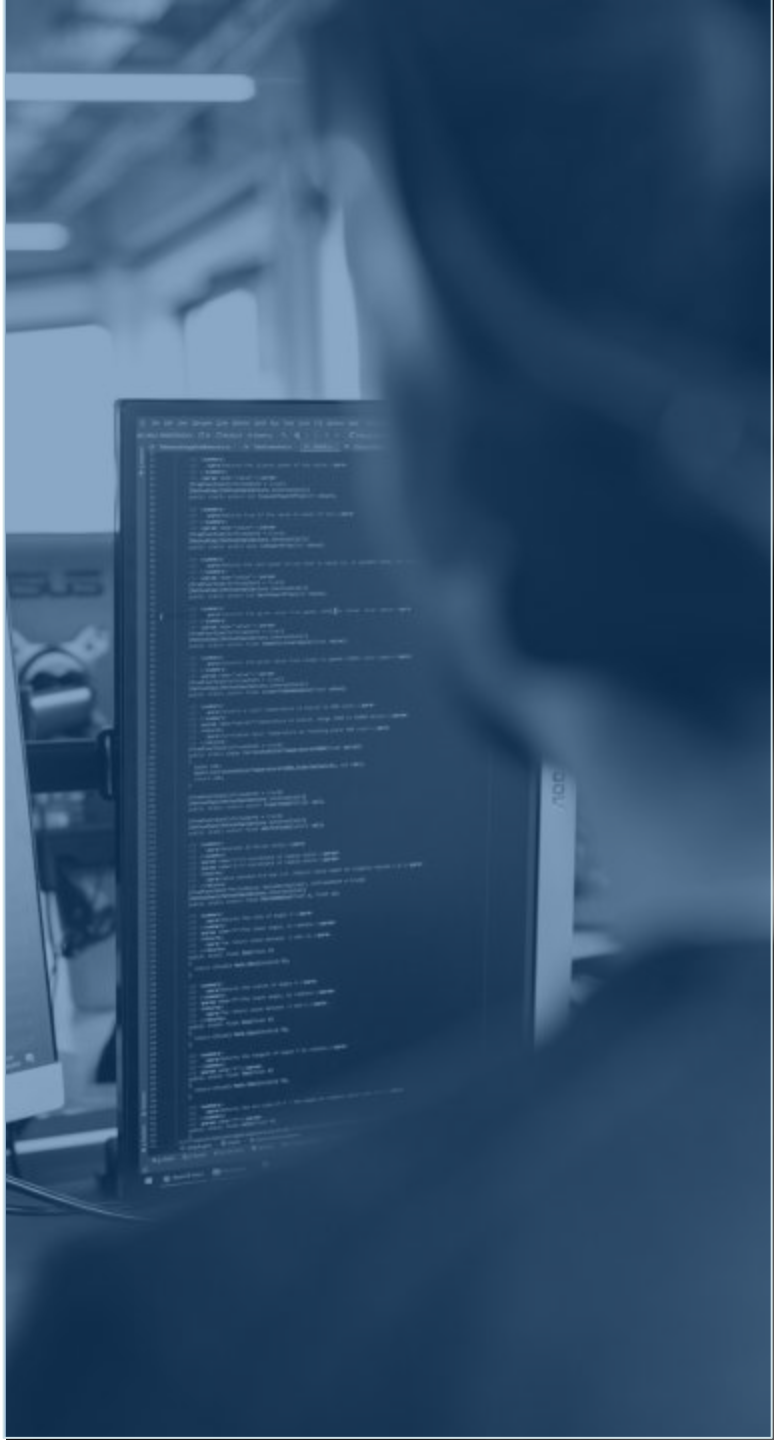
March, 2022

Powered by CYBEREADY

Защо това е важно

Активността в киберпространството, свързана с конфликта между Русия и Украйна, бележи огромен скок и дори и да не сме пряко свързани с конфликта, всички ние сме засегнати от него.

Всяка световна криза има своето киберизмерение и рязкото увеличаване на злонамерените фишинг имейли показва, че тази криза не прави изключение.



Какво се случва

1. И двете страни са стартирали кибератаки една срещу друга, които включват зловреден софтуер за изтриване на данни и сваляне на уебсайтове от мрежата, което пречи за легитимното им използване.
2. Ограничаването на тези атаки невинаги е успешно и те често заразяват устройства и уебсайтове, които нямат участие в конфликта. Това включва и вашите служебни или лични устройства.
3. Личните ви профили в социални мрежи също са застрашени от хакерски атаки с цел разпространение на невярна информация или зловреден софтуер.

Какво можете да направите, за да защитите мрежата у дома

Инсталирайте операционна система и актуализации за сигурност. Ако са налични такива, би трябвало на компютъра или телефона Ви да се появи известие.

Добавете втора степен на идентификация в профилите си в социалните мрежи (като Facebook, LinkedIn, Twitter и др.) и в имейл профилите си. Ако е възможно, добавете и резервен имейл акаунт.

Уведомете своите приятели и близки за това, което се случва, и ги насърчете да направят същото.

Какво можете да направите, за да защитите нашата мрежа

Ние сме се заели със сигурността на вътрешната мрежа, така че от техническа гледна точка не е необходимо да правите нищо.

По време на такива периоди е възможно да сте обект на повече фишинг атаки. Внимавайте, когато получавате имейли, изискващи вашето съдействие по технически или финансови въпроси.

Винаги проверявайте имейл адреса на подателя – запомнете, че това е най-важната стъпка за установяване на фишинг атака.