CYBERPRZESTĘPSTWA

01.

Czym jest cyberprzestępczość?

Cyberprzestępczość to przestępczość w zakresie działań skierowanych przeciwko systemowi komputerowemu i czynów dokonanych przy użyciu komputera jako narzędzia.

02.

Przestępczość komputerowa

Przestępczość komputerowa obejmuje wszelkie zachowania przestępcze związane z funkcjonowaniem elektronicznego przetwarzania danych, polegające zarówno na naruszaniu uprawnień do programu komputerowego, jak i godzące bezpośrednio w przetwarzaną informację, jej nośnik i obieg w komputerze oraz cały system połączeń komputerowych, a także w sam komputer, a także skierowane przeciwko takiemu systemowi.

Zadanie finansowane ze środków pochodzących z budżetu państwa z części będącej w dyspozycji wojewodów, przez udzielanie dotacji celowej powiatom, polegające na prowadzeniu punktu nieodpłatnego poradnictwa obywatelskiego w Powiecie Płockim w 2025 r.

Mazowszerazem

Ministerstwo Sprawiedliwości

03. Rodzaje cyberprzestępstw

W polskim porządku prawnym nie ma jednego aktu prawnego, który umożliwiałby organom ścigania walkę z cyberprzestępczością. Niemniej jednak regulacje dotyczące przestępczości internetowej możemy znaleźć w kodeksie karnym, a także w przepisach karnych różnych ustaw. Biorąc to pod uwagę można wyróżnić kilka typów cyberprzestępczości, które występują w polskim prawie:

04. Nielegalny dostęp do systemu (hacking)

art. 267 § 1 i 2 k.k. Hacking polega na uzyskaniu przez osobę trzecią bezprawnego dostępu do informacji lub systemu informatycznego, poprzez podłączenie się do sieci telekomunikacyjnej, przełamanie lub ominięcie zabezpieczeń elektronicznych, lub informatycznych. Przestępstwo to ścigane jest na wniosek poszkodowanego. Grozi za nie kara grzywny, kara ograniczenia wolności lub pozbawienie wolności do 2 lat.

05. Naruszenie tajemnicy komunikacji (sniffing)

art. 267 § 3 k.k. Sniffing to przestępstwo, które polega na wykorzystaniu specjalnego oprogramowania umożliwiającego bezprawne uzyskanie informacji, do których sprawca nie jest uprawniony. Poufne informacje pozyskiwane są za pomocą programów zwanych snifferami, które umożliwiają przechwytywanie danych, w tym haseł i identyfikatorów użytkowników. Za taki czyn grozi maksymalnie do 2 lat pozbawienia wolności.

06. Naruszenie integralności danych (wirusy, robaki, trojany)

art. 268 k.k., art. 268a k.k. Zniszczenie, uszkodzenie, usunięcie lub zmiana zapisu istotnej informacji, a także uniemożliwienie lub znaczne utrudnienie osobie uprawnionej zapoznanie się z nią, stanowi przestępstwo zagrożone w polskim prawie karą grzywny, ograniczenia wolności albo pozbawienia wolności do lat 2.

07. Wytwarzanie narzędzi hakerskich

art. 269a k.k., art. 269b k.k. Za popełnienie tego przestępstwa grozi kara od 3 miesięcy do 5 lat pozbawienia wolności.

08. Phishing

to jedna z najczęściej wykorzystywanych przez hakerów metod pozyskiwania danych osobowych umożliwiających włamanie się na konta bankowe ofiar. Zazwyczaj ma postać wiadomości SMS lub e-mail zawierającej link do strony internetowej przypominającej stronę banku. Celem takiej wiadomości jest wyłudzenie loginu i hasła do konta bankowego, numeru karty kredytowej oraz bezpośredniego dostępu do rachunku bankowego. Zgodnie z polskim prawem za phishing grozi kara pozbawienia wolności od 3 miesięcy do 5 lat.