Zasady bezpiecznych rozmów

Wstęp

Wiadomości są podstawowym sposobem komunikacji zarówno w życiu osobistym, jak i zawodowym. Często osobami, które stwarzają największe niebezpieczeństwo podczas pisania, jesteśmy my sami. Poznaj najczęstsze błędy popełniane przez ludzi i dowiedz się, jak możesz ich uniknąć.

Autouzupełnianie

Automatyczne uzupełnianie to powszechna funkcja wielu aplikacji. Gdy wpiszesz imię i nazwisko osoby, do której chcesz wysłać wiadomość, aplikacja może automatycznie wybrać tę osobę. Ta funkcja może prowadzić do błędów, zwłaszcza gdy wiele kontaktów podobnie się nazywa. Wiadomość, która miała trafić do współpracownika, może zamiast tego trafić do trenera, który ma bardzo podobne nazwisko. Zawsze dokładnie sprawdź dane osoby, do której chcesz wysłać wiadomość, zanim naciśniesz „wyślij”.

Odpowiadanie na wiadomości grupowe

Czaty grupowe są bardzo popularne, ale zanim zaczniesz się w nich udzielać, upewnij się, że znasz wszystkich członków grupy biorących udział w rozmowie. Wysyłane wiadomości muszą być odpowiednie dla wszystkich osób w tej grupie. Częstym błędem jest przypadkowe odpowiadanie wszystkim członkom grupy zamiast konkretnej osobie. Nie spiesz się z odpowiedzią: Sprawdź swoją wiadomość zanim ją wyślesz.

Emocje

Unikaj wysyłania wiadomości, gdy jesteś zły lub zdenerwowany. Ta wiadomość może wyrządzić ci krzywdę w przyszłości. Zamiast tego poświęć chwilę i spokojnie uporządkuj swoje myśli. Jeśli *nie możesz się powstrzymać,* otwórz nową wiadomość bez wybranego odbiorcy, napisz dokładnie, co czujesz, a następnie odejdź od komputera. Dobrym pomysłem może okazać się wyjście na spacer. Kiedy wrócisz, usuń wiadomość i zacznij od nowa. Prawdopodobnie będziesz wtedy spokojniejszy. Bezpośrednia rozmowa przez telefon lub na żywo będzie bardziej efektywna. Ludziom może być trudno określić ton i intencje w samej wiadomości tekstowej.

Prywatność

Tradycyjnym wiadomościom SMS brakuje zabezpieczeń prywatności; po wysłaniu tracisz kontrolę nad wiadomością. Wiadomości mogą być przesyłane dalej, publikowane i udostępniane w postaci zrzutów ekranu. W ważnych sprawach najlepszy może okazać się telefon do danej osoby. Jeśli używasz urządzenia służbowego do wysyłania wiadomości, pamiętaj, że pracodawca może mieć prawo do monitorowania i potencjalnego odczytywania wiadomości na urządzeniach, z których korzystasz.

Złośliwe wiadomości

Podobnie jak w przypadku poczty elektronicznej, cyberprzestępcy próbują oszukiwać za pomocą SMS-ów. Wiadomości te mogą zawierać złośliwe linki, prośby o udostępnienie danych osobowych lub naciski, abyś nawiązał kontakt z daną osobą inną drogą. Czy kiedykolwiek otrzymałeś dziwną wiadomość tekstową zawierającą tylko słowo „Cześć" i zastanawiałeś się, o co chodzi? Oznacza to, że cyberprzestępca próbuje rozpocząć z Tobą rozmowę, co często jest początkiem oszustwa nigeryjskiego. Jeśli otrzymasz dziwne lub podejrzane wiadomości, po prostu je usuń.

Ponadto, podobnie jak w przypadku e-maili, możliwe jest sfałszowanie źródła wiadomości SMS. Zanim udostępnisz jakiekolwiek dane, upewnij się, że znasz osobę, z którą piszesz, zwłaszcza jeśli nie jesteś inicjatorem rozmowy. Możesz także zablokować niechciane lub podejrzane numery telefonów.

Bezpieczeństwo wiadomości

Upewnij się, że aplikacja do przesyłania wiadomości, której używasz, jest zaktualizowana. Dedykowane aplikacje do bezpiecznego przesyłania wiadomości, takie jak Signal, zapewniające większe bezpieczeństwo i prywatność.

Redaktor gościnny

Michele Tomasic, Women in Cybersecurity (WiCyS), zastępca dyrektora, jest liderką zaangażowaną w rozwój kobiet w dziedzinie cyberbezpieczeństwa. Dzięki doświadczeniu w zarządzaniu ludźmi i zarządzaniu operacyjnym wykorzystuje swoją wiedzę, aby promować różnorodność i wzmacniać pozycję kobiet na stanowiskach pracy zajmujących się cyberbezpieczeństwem.

Źródła

Bezpieczeństwo urządzeń mobilnych: https://www.sans.org/newsletters/ouch/securing-mobile-devices/
Utylizacja urządzeń mobilnych: https://www.sans.org/newsletters/ouch/disposing-mobile-devices/
Najczęstsze błędy w e-mailach: https://www.sans.org/newsletters/ouch/avoid-the-most-common-email-mistakes/
Signal: https://signal.org

Polski przekład CERT Polska: Bartłomiej Wnuk, Aleksandra Węgrzynowicz