Telefonia mobilna

- *1G (generacja) – oparte o sygnał analogowy;*
- *2G – obsługuje połączenia telefoniczne, krótkie wiadomości tekstowe i niewielkie ilości danych w protokole o nazwie MMS*
  GSM (Global System for Mobile Communications) – usługi związane z transmisją głosu, danych oraz wiadomości w formie tekstowej lub multimedialnej.
- *3G – umożliwia jeszcze przegląd stron HTML, oglądanie filmów i słuchanie muzyki*
  UMTS (Universal Mobile Telecommunications System)

Telefonia mobilna

- *LTE (Long Term Evolution) – poprawa prędkości bezprzewodowych łączy w celu zaspokojenia rosnącego popytu*
- *4G – około pięć razy szybsza niż 3G, maksymalna prędkość pobierania 100 Mb/s*
- *5G ma być około trzy razy szybsze niż 4G, zapewniając transmisję na minimalnym poziomie 450 Mb/s aż do 10 000 Mb/s.*

Łączność bezprzewodowa

- *Bluetooth – technologia bezprzewodowej komunikacji krótkiego zasięgu pomiędzy różnymi urządzeniami elektronicznymi, takimi jak klawiatura, komputer, laptop, telefon itp.*
- *Standard IEEE 802.15*
- *Częstotliwość 2,4 GHz;*
- *Szybkość do 2,1 Mb/s*

NFC

- ***NFC*** *(near-field communication) – krótkozasięgowy standard komunikacji bezprzewodowej pozwalający na wymianę danych na odległość do 20 centymetrów.*
- *Dosyć niska szybkość transferu danych do 400 kb/s.*
- *Odczytywanie znaczników NFC.*
- *Przesyłanie danych między urządzeniami.*
- *Inicjowanie zaplanowanych działań.*
- *Płatności zbliżeniowe.*

Netykieta

- ***Netykieta jest to zbiór zasad kultury obowiązującej wszystkich(!) w Internecie.***
- ***Służyć ma uświadomieniu bądź przypomnieniu pewnych zasad obowiązujących w społeczności internautów.***
- ***3 główne zasady:***
  - Myśl!
  - Nie działaj na czyjąś szkodę!
  - Nie nadużywaj!

E-mail

- Odbieraj pocztę codziennie.
- Pisz listy w formacie tekstowym, a nie HTML.
- Nie przesyłaj pocztą elektroniczną dużych plików.
- Gdy rozsyłasz pocztę do grupy osób, korzystaj z pola BCC czyli UDW (Ukryty do Wiadomości), gdyż nie każdy sobie życzy by jego adres e-mail został ujawniony innym adresatom.
- Dostosuj formę wiadomości do statusu odbiorcy.
- Zawsze podpisuj wysyłane wiadomości.

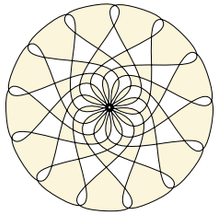
Netykieta

Komentarze i dyskusje

- Pisz rzeczowo i konkretnie, tak ażeby każdy Cię zrozumiał.
- Nie obrażaj nikogo.
- Zanim publicznie kogoś ocenisz w jakikolwiek sposób, przemyśl to na spokojnie i dwukrotnie.
- Unikaj wpisów mocno nacechowanych emocjonalne.
- Pamiętaj, że w Internecie nikt nie jest anonimowy!

Część 10

Bezpieczeństwo informacji



Marta Tyran-Kamińska

Zagrożenia

- *Zagrożenia fizyczne.*
  - Awaria sprzętu.
  - Przypadkowe lub zamierzone uszkodzenie/zniszczenie sprzętu.
  - Utrata (zgubienie lub kradzież) sprzętu.
- *Zagrożenie danych.*
  - Nielegalne kopiowanie informacji.
  - Działanie szkodliwych programów.
  - Kradzież lub uszkodzenie informacji.

Przeciwdziałania

- *Archiwizacja - tworzenie kopii zapasowych.*
- *Bezpieczne przechowywanie kopii zapasowych.*
- *Stosowanie programów antywirusowych.*
- *Instalowanie wyłącznie programów pochodzących z zaufanych źródeł.*
- *Unikanie stron www, które żądają zainstalowania dodatkowego, niesprawdzonego oprogramowania (np. nietypowych wtyczek), czy logowania, bez protokołu HTTPS*
- *Fizyczna likwidacja danych przed ”złomowaniem” nośników (płyt CD, DVD, HD, itp).*

Konfiguracja komputera

- *Konto z uprawnieniami administratora stosować tylko, do konfiguracji komputera i instalowania programów.*
- *Dla wszystkich użytkowników korzystających z komputera tworzyć oddzielne konta standardowe (z ograniczonymi uprawnieniami).*
- *Chronić wszystkie konta mocnymi hasłami.*
- *Zainstalować zaporę osobistą, ochronę antywirusową, antyspamową oraz przed oprogramowaniem typu „spyware”.*
- *Wyłączyć tryb HTML otwierania wiadomości e-mail w programie obsługującym pocztę.*

WiFi - Zasady bezpieczeństwa

- *Do zarządzania siecią WiFi należy używać połączenia przewodowego.*
- *Ograniczyć moc transmisji.*
- *Wyłączać router gdy nie jest używany.*
- *Stosować filtrowanie adresów MAC.*
- *Stosować szyfrowanie WPA2 (Wi-Fi Protected Access).*
- *Stosować długie hasła.*

Zasady tworzenia haseł

Nie należy używać

- nazw użytkowników jako hasła (np. admin, admin1),
- informacji związanych z własną osobą np. imion, nazwisk, dat urodzin,
- nazw własnych ani słów języka naturalnego,
- tego samego hasła do różnych serwisów.

Każde hasło powinno

- składać się z małych i wielkich liter, cyfr i znaków specjalnych,
- wyglądać jak losowy ciąg znaków,
- być długości co najmniej 8 znaków; czym dłuższe hasło tym trudniej je złamać.

Nie zapamiętywać haseł w systemie

Złośliwe oprogramowanie

- *Wirusy, robaki, trojany, spyware, ransomware*
- *Wirus – w ogólności segment programu, który dokleja się do innych programów w systemie,*
- *reprodukuje się wyłącznie w zasobach lokalnych danego komputera,*
- *nie może samodzielnie atakować innych maszyn,*
- *może się dostać do innego komputera poprzez płytę CD, pendrive lub zainfekowany plik w załączniku wiadomości e-mail,*
- *dokonuje aktów wandalizmu*

Robak

- *niezależny program, który rozpowszechnia się w sieci,*
- *transmituje własne kopie po sieci,*
- *sam się powiela lub dokonuje aktów wandalizmu,*
- *załączniki e-maili, strony z udostępnianymi plikami, linki do zainfekowanych stron www,*
- *zużywa dużą ilość pamięci komputerowej,*
- *lub obciąża przepustowość, urządzenia przestają reagować na polecenia.*

Trojan

- *nazwa pochodzi od konia trojańskiego,*
- *udaje, że jest użyteczny lub pomocny,*
- *w rzeczywistości uszkadza komputer i kradnie dane,*
- *zainfekowany komputer może działać wolniej z powodu obciążenia procesora,*
- *rozprzestrzenia się za pośrednictwem zainfekowanego załącznika e-mail,*
- *lub jest częścią pobieranych plików z darmowymi grami, aplikacjami, filmami i kartkami z życzeniami.*

Spyware

- *program szpiegujący; spy – szpieg,*
- *gromadzi informacje o użytkowniku: jego zwyczaje w Internecie, czy poufne dane,*
- *korzysta z Internetu, aby przekazać te informacje osobom trzecim bez wiedzy użytkownika,*
- *np. keylogger wysyła na wskazany adres informację o każdym wciśnięciu klawisza,*
- *na ogół powiązany z innym oprogramowaniem, np. przy pobieraniu darmowej muzyki lub filmów,*
- *może też być instalowane podczas otwierania załączników e-mail.*

Ransomware

- *odbiera dostęp do plików poprzez ich zaszyfrowanie; ransom – okup,*
- *po ataku, w zamian za przywrócenie dostępu do danych, przestępcy żądają zapłaty okupu,*
- *atakujący umieszczają złośliwy odnośnik lub załącznik w wiarygodnej, lecz fałszywej wiadomości e-mail,*
- *zaszyfrowane zostają dokumenty, fotografie, pliki projektowe, wrażliwe dane przedsiębiorstwa, itp.*
- *potencjalnym celem ataku może stać się zarówno firma, jak i osoba prywatna*

Physhing

- *typ ataku – za pomocą specjalnie spreparowanych wiadomości przestępcy nakłaniają ofiarę do wykonania określonej czynności,*
  - otwarcie zainfekowanego załącznika,
  - podanie hasła na niezaufanej stronie,
  - kliknięcie w złośliwy link,
- *wiadomości te wzbudzają zaciekawienie, pożądane emocje i chęć podjęcia natychmiastowego działania,*
- *wyłudzanie prywatnych danych (np. haseł do kont bankowych lub witryn internetowych, numerów kart kredytowych),*
- *Trojan oraz ransomware w kampanii podszywającej się pod InPost*

Portale społecznościowe

- *Udostępnianie zbyt wielu informacji o swoich zamierzeniach i planach.*
- *Udostępnianie zbyt wielu informacji o sytuacji materialnej.*
- *Lekceważenie ochrony wizerunku własnego i innych osób.*
- *Internet nie zapomina!!!*

  Najlepiej założyć:

  Cokolwiek co umieszczamy w sieci stanie się kiedyś dostępne publicznie.

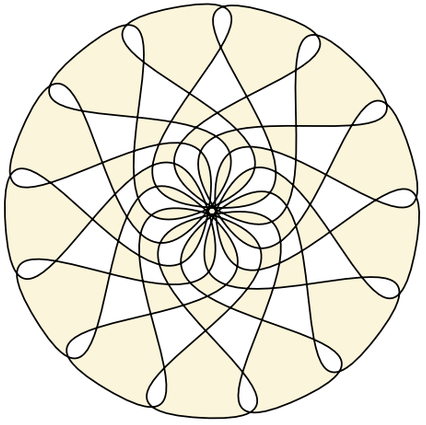
CERT

- *CERT (Computer Emergency Response Team) – Grupa Reagowania w Nagłych Wypadkach Komputerowych,*
- *utworzona w listopadzie 1988 po pierwszym ataku robaka w Internecie,*
- *internetowy „strażnik" bezpieczeństwa.*
- *Obowiązki:*
  - analiza problemów związanych z bezpieczeństwem,
  - wydawanie ostrzeżeń związanych z bezpieczeństwem,
  - prowadzenie kampanii uświadamiających w celu zwiększenia bezpieczeństwa Internetu.
- *CERT Polska jest częścią NASK,*
- *Kampania STÓJ.POMYŚL.POŁĄCZ.*

Korzystano z

- *Wikipedia*
- *CERT Polska*
- *NASK*

Koniec



Narzędzia: LaTeX, `wrapfig`, `texpower`
Rysunki: *Inkscape*