Digitální gramotnost

Kyberbezpečnost

Určeno pro distanční výuku

Obsah

Vysvětlivka k piktogramům:

 Základní informace

 Motivace pro studium tématu.

 Otázka k porozumění tématu.

 Samostatný úkol.

 Důležitá informace

1 Úvod

1.1 Kyberbezpečnost

Kyberbezpečnost je oblast, která se zaměřuje na ochranu počítačových systémů, sítí a dat před neoprávněným přístupem, zneužitím a poškozením. V dnešní digitální době je kyberbezpečnost stále důležitější, protože stoupá počet kybernetických hrozeb a útoků.

Příklad 1: Malware (škodlivý software) - Malware je počítačový program vytvořený s úmyslem způsobit škodu. To může zahrnovat viry, trojské koně, ransomware nebo spyware. Při otevření podezřelých e-mailových příloh, kliknutí na podezřelé odkazy nebo stahování neznámých souborů se může dostat malware do vašeho zařízení.

Příklad 2: Phishing - Phishing je technika, kdy útočníci se snaží získat citlivé informace, jako jsou hesla, bankovní údaje nebo osobní údaje, tím, že se vydávají za důvěryhodné osoby nebo organizace. Například přijde vám podezřelý e-mail, který tvrdí, že je od vaší banky, a žádá vás, abyste aktualizovali své přihlašovací údaje na falešné webové stránce.

Příklad 3: DDoS útok (Distributed Denial of Service) - Při DDoS útoku útočníci zaplaví cílovou síť nebo webovou stránku obrovským množstvím přístupových požadavků, což vede k jejímu přetížení a nemožnosti normálního fungování. DDoS útoky často využívají tzv. botnety, tedy sítě infikovaných počítačů, které jsou pod kontrolou útočníka.

Jaké kroky bys podnikl/a pro ochranu svého počítače a dat před kybernetickými hrozbami?

Pročti si na internetu informace o různých typech kybernetických útoků a vyber si jeden konkrétní příklad. Popiš, jakým způsobem by mohl tento útok ohrozit bezpečnost tvého počítačového systému a jak by se dal předcházet.

1.2 Pravidla slušného chování na internetu

Slušné chování na internetu je základním principem pro vytvoření příjemného a respektujícího prostředí online. Zde je několik pravidel, která bychom měli dodržovat:

Příklad 1: Respektuj ostatní: Buď zdvořilý/á a ohleduplný/á k ostatním uživatelům. Nepoužívej vulgární nebo urážlivý jazyk a neposílej nevhodný obsah. Například, když se účastníš diskuse na sociální síti, buď opatrný/á s tím, co píšeš, a vyjádři svůj názor v respektujícím tónu.

Příklad 2: Chrání soukromí: Dodržuj soukromí ostatních lidí. Neposílej jejich osobní informace bez jejich souhlasu a neporušuj jejich důvěru. Například, pokud někdo sdílí osobní informace nebo problémy na internetu, respektuj jeho/její soukromí a neposkytuj tyto informace dalším lidem.

Příklad 3: Respektuj autorská práva: Nezveřejňuj nebo nešiři materiály, které mají autorská práva bez souhlasu vlastníka. Například, pokud najdeš zajímavý článek nebo obrázek na internetu, uveď zdroj nebo požádej o povolení, pokud chceš použít tento materiál ve svém vlastním obsahu.

Jaké jsou podle tebe nejdůležitější zásady slušného chování na sociálních sítích?

Přemýšlej o situacích, ve kterých by mohlo dojít k porušení pravidel slušného chování na internetu. Navrhněte konkrétní kroky, jak byste mohli reagovat na tyto situace a předejít nevhodnému chování.

2 Závěr

Kyberbezpečnost a slušné chování na internetu jsou nezbytné pro bezpečné a příjemné online prostředí. Zajištění kyberbezpečnosti a dodržování pravidel slušného chování je zodpovědností každého uživatele internetu. Vždy si uvědomujme důležitost chránit naše osobní údaje, respektovat soukromí ostatních a jednat slušně v online komunitách.

3 Seznam doporučených zdrojů a literatury

Knihy:
Anderson, R., & Moore, T. (2019). Bezpečnost počítačových sítí: pro profesionály a nadšence. Computer Press.

Schneier, B. (2015). Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. W. W. Norton & Company.

Peltier, T. R. (2016). Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security Management. Auerbach Publications.

Online zdroje:
National Cyber Security Alliance (NCSA): https://staysafeonline.org/
National Institute of Standards and Technology (NIST) Cybersecurity Framework: https://www.nist.gov/cyberframework
European Union Agency for Cybersecurity (ENISA): https://www.enisa.europa.eu/
Cybersecurity and Infrastructure Security Agency (CISA): https://www.cisa.gov/
Vědecké články a publikace:
Whitty, M. T., & Carr, A. N. (2006). Cyberspace romance: The psychology of online relationships. Palgrave Macmillan.
Dinev, T., & Hart,

4 Testové otázky

Otázka 1: Co je kyberbezpečnost?
a) Ochrana počítačových her
b) Ochrana počítačových systémů, sítí a dat před neoprávněným přístupem a poškozením
c) Bezpečnost kybernetických robotů

Otázka 2: Jaké jsou důsledky malware?
a) Zlepšení výkonu počítače
b) Ztráta dat, omezení funkčnosti systému nebo zneužití osobních údajů
c) Vytvoření virtuální reality

Otázka 3:
Co je phishing?
a) Technika získávání ryb
b) Útok na webovou stránku
c) Útok, kdy se útočníci vydávají za důvěryhodné osoby nebo organizace s cílem získat citlivé informace

Otázka 4: Jaká pravidla platí pro slušné chování na internetu?
a) Respektovat soukromí ostatních, chránit osobní údaje a respektovat autorská práva
b) Sdílet osobní informace bez souhlasu ostatních
c) Vyhledávat informace bez omezení

Otázka 5: Co je nevhodné chování na sociálních sítích?
a) Respektování názorů a ochrana soukromí
b) Používání vulgárního jazyka a šíření nevhodného obsahu
c) Odpovídání na zprávy ve vhodném časovém rozmezí

Klíč:
b
b
c
a
b