NIE BĄDŹ G(Ł)UPIK.

PHISHING

MALWARE

RANSOMWARE

NIE DAJ SIĘ ZŁOWIĆ CYBERPRZESTĘPCOM!

Phishing, malware, ransomware - jak się zabezpieczyć przed tymi zagrożeniami? 💻
Oto kilka podstawowych zasad:

NIE ŁAP SIĘ NA HACZYKI:

- **NIE PODAWAJ** swoich danych osobowych lub finansowych na stronach internetowych, które nie są zabezpieczone protokołem HTTPS lub mają podejrzany adres.
- **NIE PODŁĄCZAJ** dysków zewnętrznych, jeśli nie masz pewności, że są bezpieczne.
- **NIE KLIKAJ** w podejrzane przynęty: w wiadomościach e-mail, SMS lub na komunikatorach – to może być WĘDKOWIRUS. 🎧
- **NIE LOGUJ SIĘ** do banku przez publiczne WIFI.

ABY UNIKNĄĆ ZŁOWIENIA W SIECI🐠:

- **UŻYWAJ SILNYCH HASEŁ** i autoryzacji dwuetapowej: Wybieraj unikalne, trudne do złowienia hasła dla każdego konta online. Dodatkowo, jeśli to możliwe, włącz autoryzację dwuetapową, która dodatkowo zabezpieczy Twoje konto.
- **UŻYWAJ AKTUALNEGO OPROGRAMOWANIA** antywirusowego i zapory sieciowej na swoim komputerze lub urządzeniu mobilnym.
- **REGULARNIE TWÓRZ KOPIE ZAPASOWE** swoich ważnych plików na zewnętrznym nośniku lub w chmurze.
- **BĄDŹ ŚWIADOMY** technik inżynierii społecznej, które mogą być używane przez oszustów do wykorzystywania twojego zaufania. 🧠

#CyberBezpieczeństwo #WiedzaJestSila #NieBadzGlupikNieDajSieZlowic