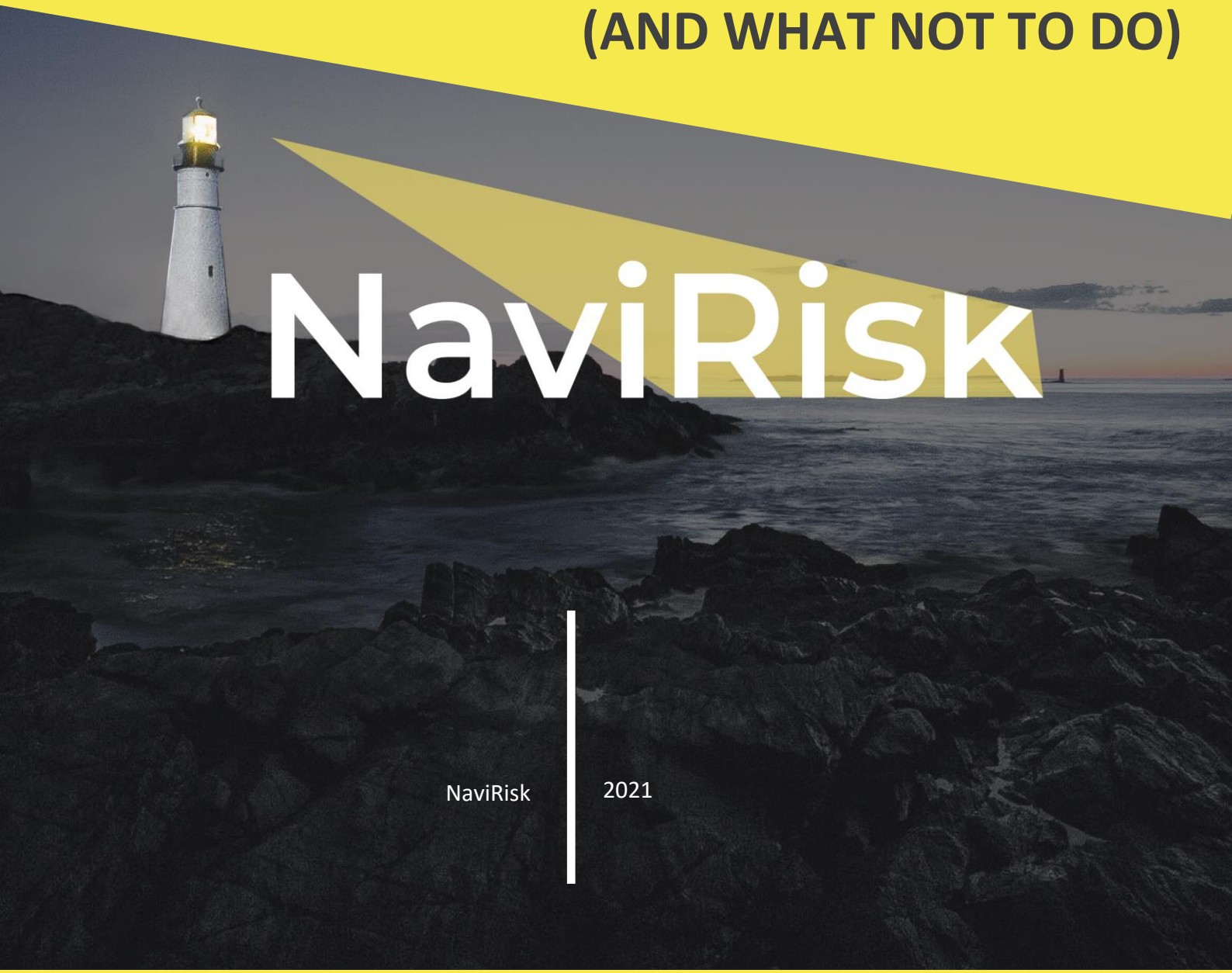
HACKER ATTACK

-

A PRACTICAL GUIDE WHAT TO DO (AND WHAT NOT TO DO)



NaviRisk

2021

DO YOU SUSPECT A HACKER HAS ATTACKED YOU?

CHECK IF YOU HAVE FOLLOWED OUR EXPERT'S RECOMMENDATIONS:

1. **Disconnect from the local network and the Internet - the attacker will lose access, but most of all, the threat will not spread to other infrastructure elements.**

2. **Notify the security and IT staff in your organization or company.**

3. **In the case of a ransomware attack (when the hacker encrypts your computer's data and demands a ransom), do not act on your own - use the services of a specialized company. Proficient experts will establish contact with the attackers, assess a given hacker group and its credibility (e.g. whether they will decrypt after the ransom has been paid), conduct professional negotiations, and perhaps recognise the malware as easy to decrypt.**

4. Do not react to suspicious pop-up windows and messages about computer viruses, computer allegedly blocked by the police, etc. That means do not click on the links posted there, do not make calls, do not enter data in suspicious forms, or by phone when you get an unexpected phone call.

5. In your computer works strange, check running processes and applications (e.g. in MS Windows Task Manager), verify established connections (e.g. in MS Windows using the "netstat - ano" command in the "cmd.exe" command panel).

6. Check all the sites and services (e.g. social networks, instant messaging apps, e-mail, CRM/ERP, MS365, entertainment, etc.), log history and the sessions currently connected and logged; block suspicious ones or log out of certain websites on some or all devices.

7. Change passwords for all services and - better late than never - where possible and not yet configured, set up multi-factor or two-factor authentication, e.g. using text message codes, an additional authentication application, consider using dongles.

8. In the case of, e.g. computer infection or a hacked e-mail account, inform your relatives, colleagues and friends to be careful and not to open e-mails or attachments from you.

9. In certain cases, notify your bank (e.g. hacking into a bank account) and the Police.

10. Report to other institutions - depending on the type of threat and its potential consequences (e.g. the police or the Personal Data Protection Office in the event of personal data leakage, when there is a risk of violating the rights and freedoms of data subjects).

11. In some instances, it may be necessary to block the SIM card or even change the phone number.

12. Decide whether to clean the environment thoroughly or secure the media and equipment as material for further analysis and possible evidence. Order computer forensics experts to secure and analyse the evidence material.

13. Last but not least, remember to implement procedures in the event of another attack or suspicious activity and ... contact us.

We will help you.

info@cyberprevent.pl or info@wearenavirisk.com

NaviRisk

CONTACT

NaviRisk

Huculska 5/6
00-730 Warsaw

+48 605 19 11 19

info@wearenavirisk.com

www.wearenavirisk.com