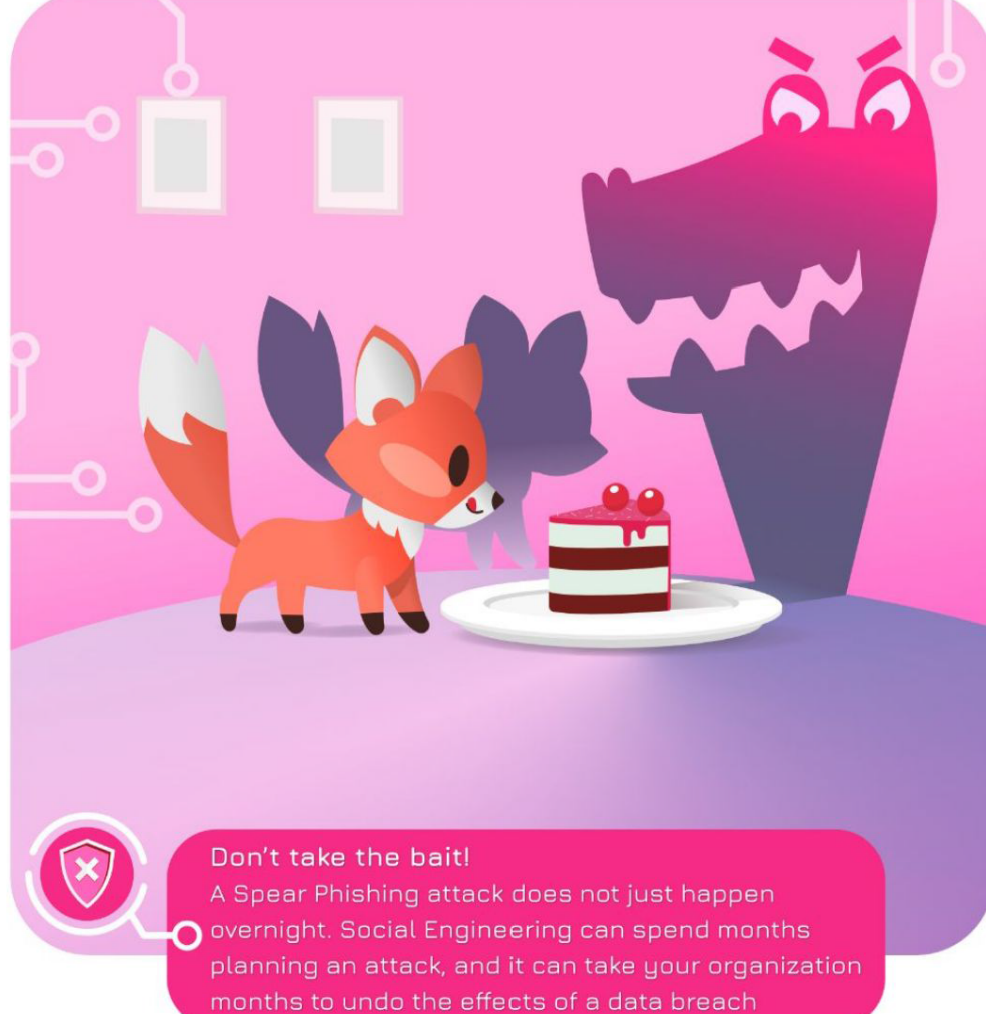


You are receiving this email because you have taken part in the IFES Regional Election Technology and Cyber-Hygiene course. This newsletter provides reminders of good cyber-hygiene practices to use in daily practice.

Following the global COVID-19 outbreak, a number of government institutions around the world have allowed their staff to work remotely. This might already include yours!

Unfortunately, the transition to mass remote working worldwide is also a golden opportunity for cyber criminals to sow chaos and make money.



**Don't take the bait!**  
A Spear Phishing attack does not just happen overnight. Social Engineering can spend months planning an attack, and it can take your organization months to undo the effects of a data breach.

Phishing is here to stay and COVID-19-themed malicious emails are the new trend!

Since the beginning of the year, phishing campaigns have been launched with new bogus emails containing links claiming to have important updates and information related to the crisis. These malicious links can lead to infections on your devices once accessed.

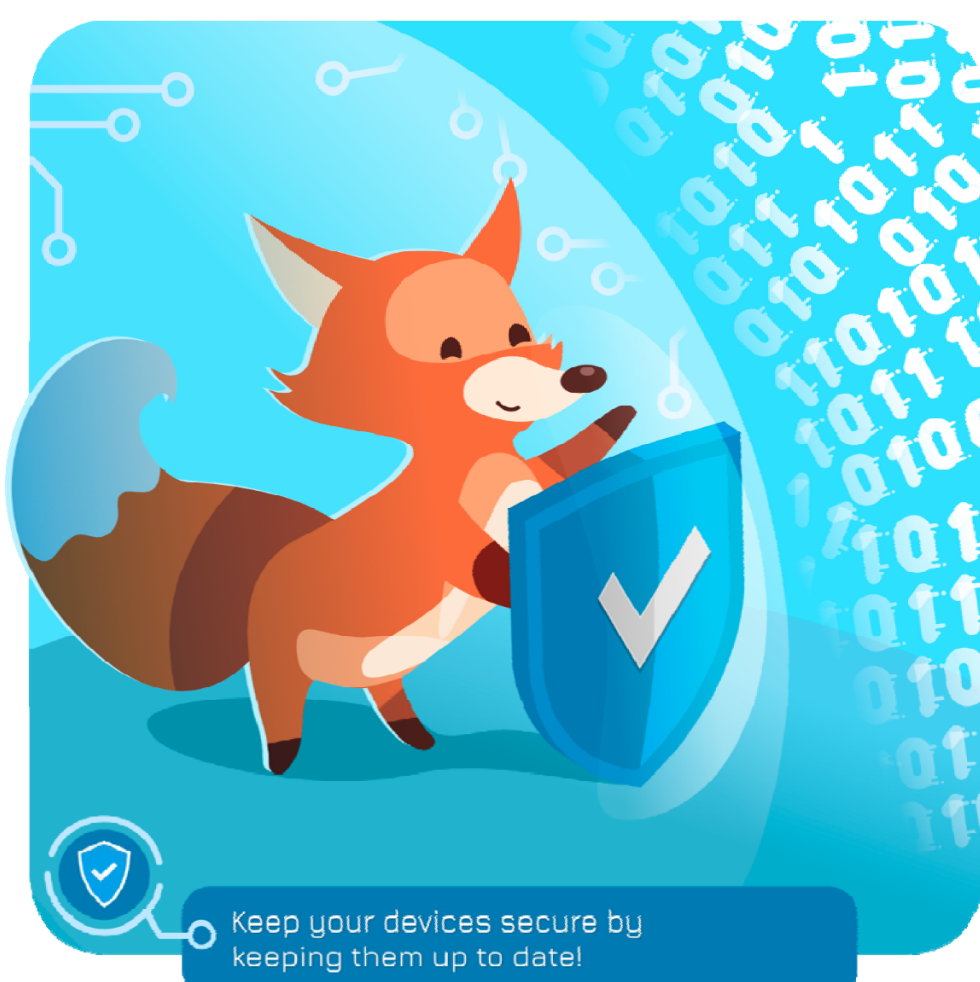
How do you spot these malicious emails?

Cyber criminals are actively trying to exploit your fears and concerns about the virus. They can also try to impersonate national health agencies. Typically, these emails can:

- Ask you to provide sensitive information such as usernames and passwords, or simply request you fill out a form with proprietary personal information that can then be exploited by more sophisticated attack vectors;
- Click on a malicious link;
- Open a malicious attachment.

What should you do?

**If you have any doubt, simply refrain from clicking the attachment or the link. Important updates and news are unlikely to come to you as an email attachment.**



**Keep your devices secure by keeping them up to date!**

Keeping your system up-to-date and running an anti-virus program are more important than ever, particularly if you are not protected by your organization's network and IT team!




Without an anti-virus program, your system might already be infected, and could endanger your personal work, the work of your colleagues and your organization as a whole. This could be due to increased bogus COVID-19 emails described above, or it could be caused by other phishing emails.

What should you do?

**Software updates offer a number of benefits! They fix security problems and bugs in both your operating system and your software. Now is the perfect time to update your operating system, install/update an anti-virus program and do a full scan of your system.**

For tips, try a Google search with the name of your anti-virus program, or you can always contact your IT support (if any), or your tech savvy colleagues. Also, it would be worthwhile to familiarize yourself with the phishing tactics outlined above and be sure to share with at least three colleagues the importance of vigilance and personal responsibility to blunt the threat.

Several relevant publications have been produced by national and international organizations alike, providing additional guidance:

-  ENISA, [Tips for Cybersecurity when working from home](#)
-  National Cyber Security Centre (NCSC, UK), [Recommendations for working from home following the Coronavirus \(Covid-19\) outbreak](#)
-  Global Cybersecurity Alliance (GCA), [Work From Home. Secure Your Business](#)

**Follow the instructions provided by your government!**

**Refer to recommendations to prevent the spread of the virus from the [WHO!](#)**

**Mental health is as important as computer health! Stay in contact (virtually) with your colleagues and your community!**

**Remember to contact your IT department if you have a question regarding remote work!**

The International Foundation for Electoral Systems' *Regional Election Administration and Political Processes Strengthening* program was designed with support from the U.S. Agency for International Development (USAID) to address common challenges among Central and Eastern European and Eurasian societies. Learn more [here](#).

