TAKE BACK CONTROL!

What to do if you responded to phishing email?

1 THINK OF WHAT DATA YOU SHARED

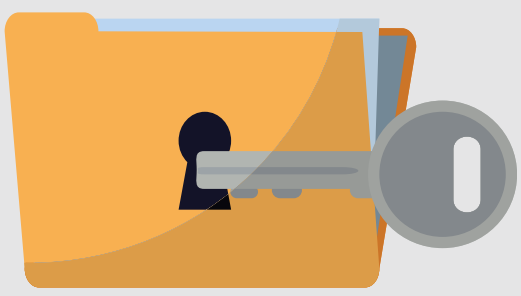
Did you recently get a notice that says your personal information was exposed in a data breach? Or learn that an online account was hacked? Is someone using your information to open new accounts or make purchases? Think of where and to whom you have provided your personal information. Did you renew an online account through an email, or responded to a message from your bank? What data did you provide? Credit card details, passwords, pin codes...

2 ONLINE LOGIN OR PASSWORD

1. **Log out of all accounts you might have open, also on your smartphone. Log into accounts and change your password. If possible, also change your username.**
2. **Just in case, change your passwords everywhere else.**
3. **Pay attention to if your card number was stored. Check your bank account for any charges that you don't recognize.**

3 DEBIT OR CREDIT CARD DETAILS

1. **Contact your bank or credit card company to cancel your card and request a new one.**
2. **Review your transactions regularly. Make sure no one misused your card.**



4 BANK ACCOUNT INFORMATION

1. **Contact your bank to close the account and open a new one.**
2. **Review your transactions regularly to make sure no one misused your account.**
3. **If you have automatic payments set up, update them with your new bank account information.**

5 REPORT AND SPREAD AWARENESS

Do not be afraid to seek help! Contact cyber.politsei.ee and cert@cert.ee, and report the incident. Your information might be helpful to uncover the scammer, seek justice and prevent others from similar incidents in the future!

LEARNING IN INTERDISCIPLINARY FOCUSED ENVIRONMENT
LIFE.