eauditor

EMPLOYEE GUIDE

Black Friday – 6 rules for safe online shopping

Before you open a link, enter your details or approve a payment, check where the request comes from.

01

Check the address and the seller

Look for typos and extra words in the web address. Check the company's details and read reviews outside its own store. A padlock alone does not prove the seller is honest.

02

Verify the offer outside the ad

Open the brand's official website yourself and look for the same promotion. A sponsored ad can also lead to a fake store.

03

Track parcels in the courier's app

Got an SMS about a surcharge or an address change? Check the shipment in the carrier's app or in your order history.

04

Protect passwords and login approvals

Use different passwords and turn on extra login verification if it is available. Reject requests to approve a login you did not start.

05

Read the payment confirmation

Check the amount, the recipient and the type of operation. Stop if the message is about anything other than the purchase you planned.

06

Report suspicious incidents

If you opened a suspicious link on a work device, tell IT. Say whether you entered data, downloaded or ran a file, or approved an operation.

Clicked a suspicious link? Report it to IT.
Even if nothing happened.

Entered your details or suspect a leak?

Password

From a trusted device, open the official service, change your password and end other sessions if the service allows it. Change it everywhere the same password was used. For a work account, contact IT right away.

Card or payment

Contact your bank right away through its app or official phone number. Block the exposed card and report suspicious transactions.

Company data or a downloaded file

Report the case to IT. Keep the message and note the time and the details you provided. Do not delete history or files and do not install repair tools on your own.

→ https://www.eauditor.eu/en/blog/what-should-you-do-after-a-security-incident

Educational and marketing material by BTC. It contains general tips and does not replace your company's incident response procedure, an individual assessment of an incident or specialist advice. Agree on further steps with IT or your bank.