News

Black Friday and Cybersecurity

Written by: Horiens - 06/11/2023

Black Friday | Do you know how to shop online safely?

Check out a quick guide to avoid falling for digital scams, becoming a victim of data theft and financial loss. Information and awareness are key steps to reducing risks.

Black Friday, a date known for retail stock clearance, usually brings good shopping opportunities not only on the official date, which in 2023 will be on 24/11, but throughout the whole month of November.

However, it's important to be careful when shopping! While discounts proliferate, the risks of shopping online also increase. Digital security experts indicate that Black Friday 2023 will be a peak time for cyber attacks.

Cyber risks are among today's main risks, affecting both individuals and companies. "Often, attacks against companies start outside of them, through employees in their personal routines on the Internet," explains Ronaldo Andrade, CISO (Chief Information Security Officer) at Horiens.

"Horiens supports companies in dealing with risks, including cyber risks. Spreading preventive information and raising awareness among employees is an essential part of a culture of prevention and information security," he adds.

We share below 10 cybersecurity tips that are valuable not only for this period but whenever you make any purchase through e-commerce.

1. Carefully check the website address for any swapped letters and ensure the URL is preceded by a padlock and the "https" acronym.
2. Do not use public networks for online shopping; always use your private network.
3. Check the store's reputation on sites such as "Reclame AQUI", "gov.br" and "Procon-SP".
4. Do not save card information in the browser or on the e-commerce site.
5. Never provide your credit or debit card password during the purchase transaction.
6. Check the value of the purchase and the shipping cost in the virtual cart before making the payment.
7. Use the card on the websites of well-known companies that you are used to buying from. Alternatively, on other sites use the option to pay by pix or boleto.
8. When using a card, prefer the "virtual card" version, which is enabled for purchases for a fixed period, reducing the risk of cloning.
9. For safer payments through mobile apps, enable identity authentication configuration by biometrics, always using a second factor of authentication.

10. Before paying bank slips, check if they are indeed authentic, verifying information from the credit operator, bank or your personal data. Also check that the receiving establishment is the same as the one you made the purchase from.

If you are the victim of any scam, file a police report at the cybercrime police station. Each state has its own police station. Below are the links for São Paulo, Rio de Janeiro, and Bahia.

SP: https://www.delegaciaeletronica.policiacivil.sp.gov.br/ssp-de-cidadao/pages/comunicar-ocorrencia/outras-ocorrencias/local-e-hora-da-ocorrencia

RJ: https://dedic.pcivil.rj.gov.br/

Bahia: https://www.delegaciadigital.ssp.ba.gov.br/OcorrenciaInternet/Bemvindo.ssp