bankinter

10 common mistakes in your company's digital security and how to avoid them.

Cybercriminals are also back for Christmas, ready to bring coal and malware into your company. Here are **10 common mistakes** and how to avoid them this Christmas:

1. Providing proxy codes to unauthorized administrative personnel.

One of the most common mistakes is to give access to proxy passwords to administrative staff. This can potentially result in unauthorized access.

How to act?

To prevent any unauthorized access, companies must have strict access control policies, storing keys centrally and controlling access to them following the principle of least privilege. In addition, it is recommended to use multi-factor authentication (MFA) for sensitive access, ensuring that only authorized people can access it.

2. Sharing credentials via email.

By sharing credentials via email, such as usernames and passwords, critical information is exposed to potential attacks. Attackers can intercept communications and gain visibility into everything we share in them.

How to act?

Divide the information, sending the username and password through different communication channels (email, call, SMS, etc.). This reduces the risk of both parts of the credentials being intercepted simultaneously by a cybercriminal. Additionally, it is advisable that the password provided is temporary, and must be changed by the recipient immediately after the first use. And, whenever possible, end-to-end encryption techniques should be applied to communications.

3. Storing coordinate cards insecurely.

Saving coordinate cards in unsecured media, such as photographs on the mobile phone, or making photocopies of them, increases the risk of information theft.

How to act?

To minimize the risks of disclosure and misuse of this information, avoid duplicating or extracting data from your coordinate card. Always keep these cards in a safe place and access them only when absolutely necessary.

4. Not verifying the suppliers' bank account.

Paying invoices without regularly checking the suppliers' checking account can lead to fraud such as depositing payments into fraudulent/attacker bank accounts.

How to act?

To avoid these frauds, it is essential that companies have mandatory verification procedures for any changes in the suppliers' bank accounts, including direct confirmation of the data with a reliable source.

5. Not confirming bank account changes over the phone.

It is important to confirm by telephone, with the appropriate interlocutor, any change of bank account. Failure to do so can allow fraudulent payments, as cybercriminals could have impersonated the legitimate recipient.

How to act?

To protect against these attacks, companies should have a validation protocol in place across multiple channels (e.g., phone calls, video conferences) before accepting changes to payment information.

6. Accepting mail orders without prior validation (CEO Fraud).

Executing orders received by mail without verifying them can lead to potential phishing attacks, such as phishing or spear phishing, where attackers pose as a legitimate person or entity to trick the victim.

These attackers usually impersonate a senior official, who, making use of his authority, transfers urgency, speed and discretion in the operation without asking questions and skipping the usual procedures.

How to act?

To avoid this, organizations should have a multi-channel verification policy for any critical data or financial action order received in the mail, including reporting mechanisms for any request that attempts to bypass the channels set forth in the policy, regardless of who the petitioner is.

7. Using weak or repeated passwords.

Low-complexity passwords make it easier for brute force attacks to succeed, allowing cybercriminals to guess them. In addition, password repetition allows attackers to access multiple accounts if a credential is compromised, exposing companies to security breaches and information theft.

How to act?

To mitigate these risks, it is essential to use strong and unique passwords for each account. Enterprises should have robust access control policies in place, preferably combined with multi-factor authentication (MFA) to add an extra layer of security.

8. Not updating software or applying security patches.

Not keeping systems up to date leaves companies vulnerable to attacks, as cybercriminals can exploit known flaws to carry out attacks of various kinds.

How to act?

It is imperative that companies implement update management policies that include the regular installation of critical security patches. In addition, it is essential to carry out regular vulnerability tests, with the aim of identifying and correcting them as soon as possible.

9. Not making regular backups or testing their restoration.

The absence of backups, or not verifying the backups that are made, exposes the company to losing crucial information in the event of a ransomware attack or a system failure.

How to act?

To avoid this risk, companies must have regular backup policies and mechanisms in place. These backups must be verified through periodic restore tests to ensure the integrity of the backed up data.

10. Not training employees in digital security.

Untrained/untrained staff are more vulnerable to phishing and malware attacks because they lack the necessary knowledge to identify and prevent threats.

How to act?

Organizations should include in their training programs continuous training and awareness in digital security, with actions that explain how to recognize threats and emphasize the importance of their identification.

At Bankinter we work continuously for your safety, if you have any questions about any situation, call our **Fraud Support Service: 900 81 00 62**.

In addition, we follow the European Directive PSD2 on payment services, so for certain transactions, **we will ask you for a password that we will send by SMS to your mobile phone**.

If you want to check that your mobile number is correctly registered, go to **bankinter.com/empresas, and access your Management Area: Users Profiles Security Signature**.

bankinter.