NAVI MUMBAI BANK

नवी मुंबई को-ऑप. बँक लि.

NAVI MUMBAI CO-OP. BANK LTD.

TOP 10 COMMON CYBERSECURITY MISTAKES EMPLOYEES MAKE AND HOW TO AVOID THEM

In today's digital age, employees play a crucial role in safeguarding their organizations from cyber threats. However, despite the growing awareness of cybersecurity best practices, common mistakes are still made, putting sensitive data at risk. To help employees stay vigilant, we prepared a list of common cybersecurity mistakes employees make, along with practical solutions to avoid them.

COMMON CYBERSECURITY MISTAKES ALONG WITH PRACTICAL SOLUTIONS

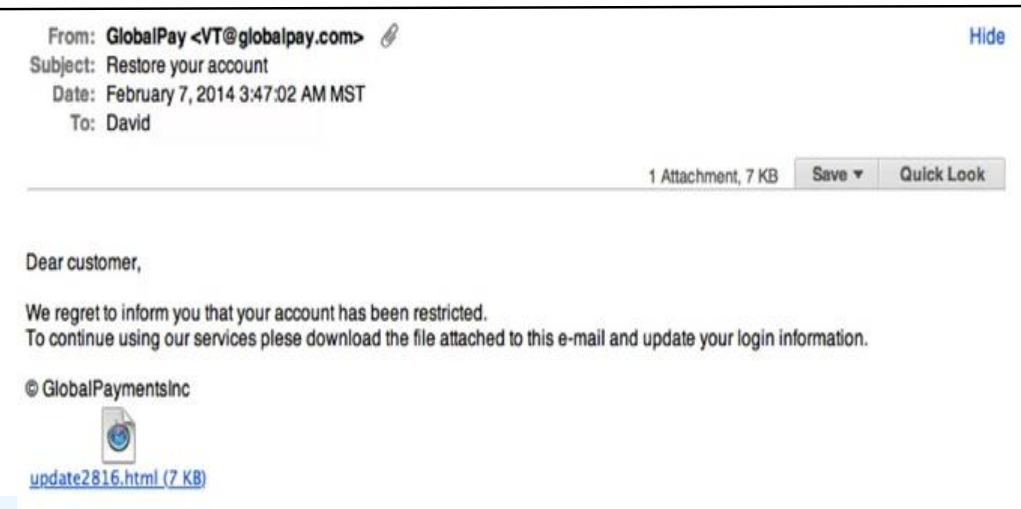
1. Weak Passwords

Mistake: Using easily guessable passwords like "*admin*" or "*password*." Some common easy to guess patters of password used in a business are -

- [orgname]@123 or [orgname]123 or [username]@birthdate
- [username]@123 or [username]123 or personal mobile number
- All employees are provided same password to access different personal systems. **Example:** All desktops have same password.

Solution: Use strong, unique passwords with a mix of letters, numbers, and symbols. Implement two-factor authentication (2FA) for an additional layer of security. **Example:** RKI&7@Y$()!dy1cqb

2. Phishing Attacks:



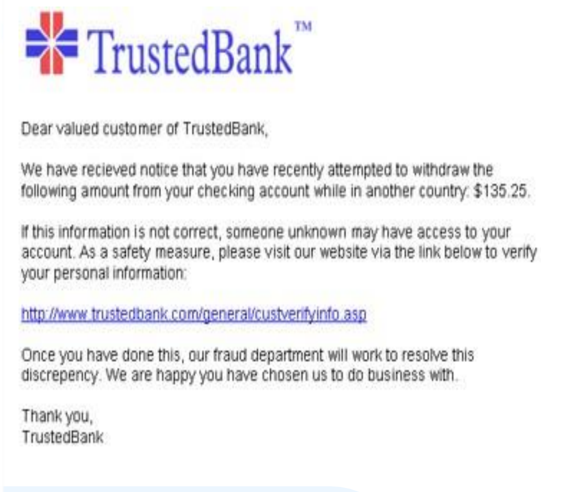
From: GlobalPay <VT@globalpay.com>
Subject: Restore your account
Date: February 7, 2014 3:47:02 AM MST
To: David

Dear customer,

We regret to inform you that your account has been restricted.
To continue using our services plese download the file attached to this e-mail and update your login information.

© GlobalPaymentsInc

update2816.html (7 KB)



Dear valued customer of TrustedBank,

We have recieved notice that you have recently attempted to withdraw the following amount from your checking account while in another country: $135.25.

If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

http://www.trustedbank.com/general/custverifyinfo.asp

Once you have done this, our fraud department will work to resolve this discrepency. We are happy you have chosen us to do business with.

Thank you,
TrustedBank

Mistake: Clicking on suspicious links in emails or downloading attachments from emails or unknown sources.

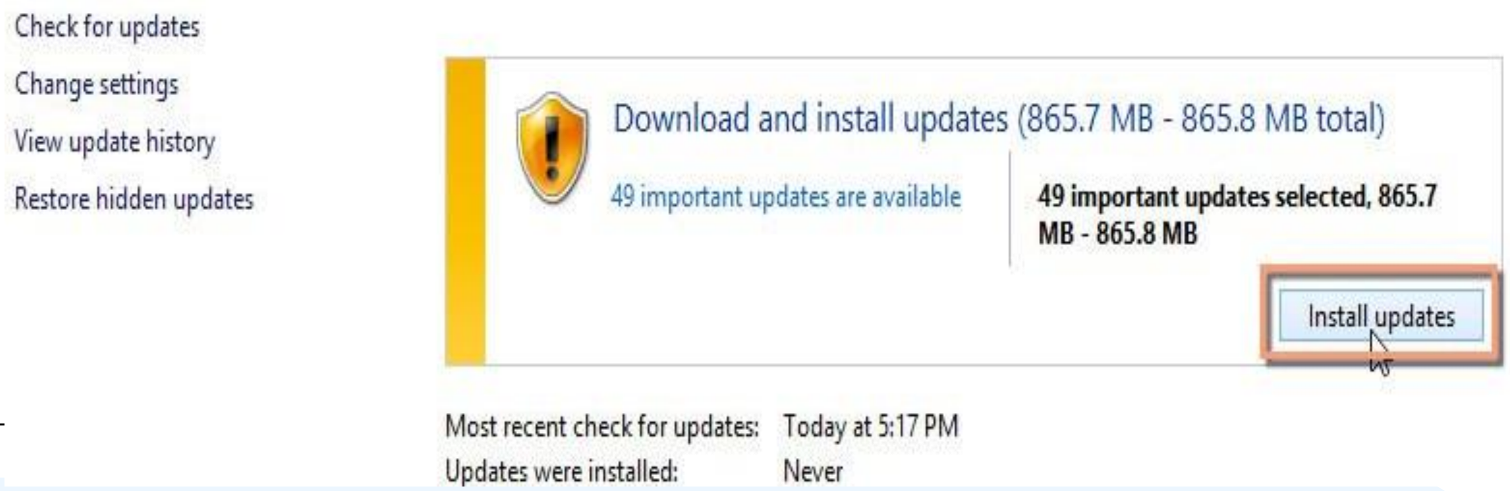
Solution: Train employees to recognize phishing attempts and provide regular awareness programs. Encourage them to verify the sender's email address and avoid clicking on unsolicited links or downloading attachments.

3. Public Wi-Fi Connections:

Mistake: Connecting to insecure public Wi-Fi networks without proper security measures.

Solution: Advise employees to use virtual private networks (VPNs) when accessing company data on public networks. Ensure they understand the risks associated with unsecured Wi-Fi and encourage the use of company-provided secure networks whenever possible.

4. Ignoring Software Updates:



Download and install updates (865.7 MB - 865.8 MB total)

49 important updates are available

49 important updates selected, 865.7 MB - 865.8 MB

Most recent check for updates: Today at 5:17 PM
Updates were installed: Never

Mistake: Delaying or ignoring software and security updates.

Solution: Remind employees to enable automatic updates for operating systems, applications, and antivirus software. Regular updates patch vulnerabilities, making it harder for cybercriminals to exploit weaknesses.

5. Careless Handling of Sensitive Information:

Mistake: Leaving sensitive documents unattended or discussing confidential matters in public spaces.

Solution: Implement a clean desk policy to ensure employees secure sensitive information when they are away from their desks. Train employees on the importance of confidentiality and maintaining privacy, both online and offline.

6. Unauthorized Device Usage:

Mistake: Using personal devices without proper authorization and security measures.

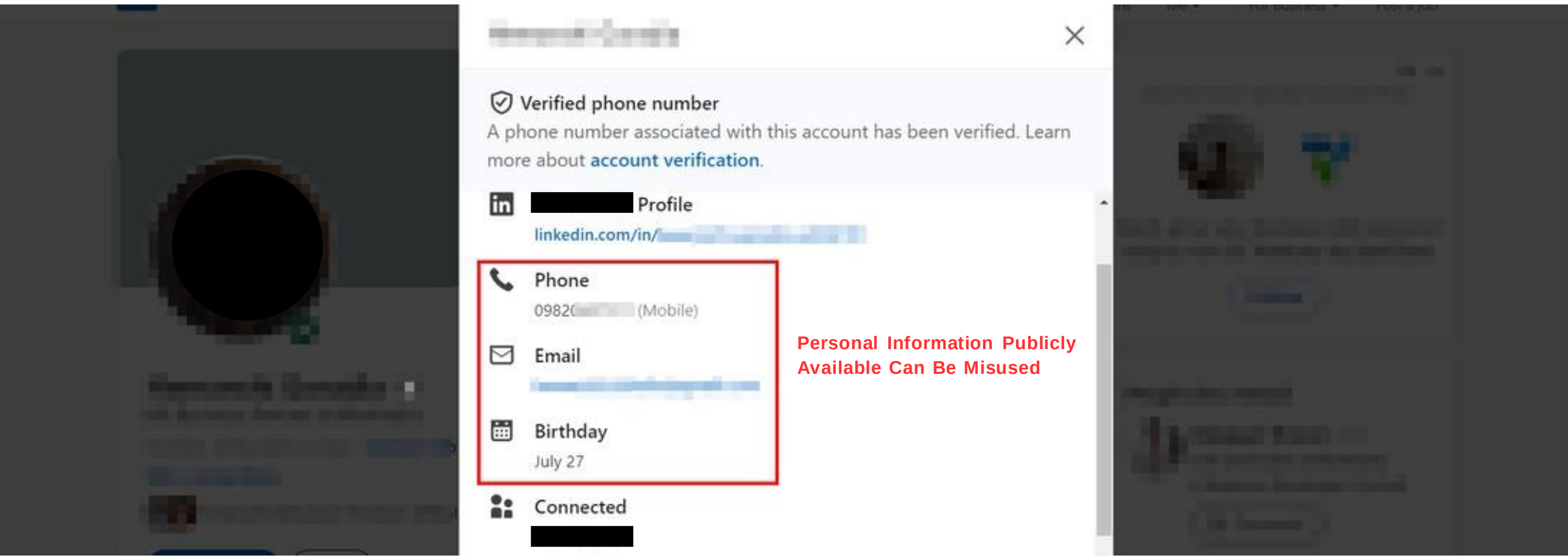
Solution: Don’t allow personal devices in sensitive premises such as IT Rooms. Mobile phones can be hacked and can be used by hackers to monitor employees while they are at work. This may disclose internal discussions within office walls, office images, calls of the employee whose phone is hacked, etc.

7. Lack of Data Backup:

Mistake: Not regularly backing up important data, making the organization vulnerable to ransomware attacks.

Solution: Encourage employees to back up their data regularly to secure, encrypted cloud storage or external drives. Automate backup processes where possible to ensure consistency.

8. Social Engineering Attacks:



Verified phone number

A phone number associated with this account has been verified. Learn more about account verification.

[redacted] Profile

linkedin.com/in/

Phone

0982 (Mobile)

Email

Birthday

July 27

Connected

[redacted]

Personal Information Publicly Available Can Be Misused

Mistake: Sharing sensitive personal or professional information over the phone, social media or email without proper verification.

Solution: Instruct employees to verify the identity of the person they are communicating with, especially if the request involves sensitive information or financial transactions. Implement strict protocols to not share any media related to office on social media as they could leak sensitive data about office premises to the hackers on the internet.

9. Unrestricted Access Rights:

Mistake: Granting employees unnecessary access to sensitive systems and data.

Solution: Implement the principle of least privilege, ensuring employeesonly have access to the information necessary for their roles. Regularly review and update access permissions based on job responsibilities and changes within the organization.

10. Failure to Report Security Incidents:

Mistake: Not reporting suspicious activities or security breaches

Solution: Foster a culture of open communication and educate employees on the importance of reporting any unusual activities or potential security incidents immediately. Establish a clear incident response protocol to handle reported incidents effectively.

THANK YOU