Information Security

Overview

At TransUnion CIBIL, we aim to provide Information for Good. With our consumers' data at the centre of our business, we strive to secure your information and ensure it is protected. However, we need your cooperation in this constant fight against fraud. Have you ever realised how easy it is to fall prey to credit fraud and identity theft?

Despite the advances in the digital world, there are innumerable ways in which you can expose your confidential information online and put yourself at risk.

Phishing Techniques

In the digital world, there are innumerable ways in which you can expose your confidential information online and put yourself at risk. Learn more about each of these techniques and how you can protect your online identity

PHISHING

Phishing is an attempt to obtain any type of sensitive or personal information such as login credentials, banking and card details or even personal identifiers (like your PAN and AADHAR number) through deceitful means, such as impersonating another in any kind of electronic communication. This is used by cyber criminals to trick users into revealing sensitive confidential data simply by luring them through ***fake emails and websites***.

Did you know that spear-phishing is a targeted cyber-attack to trick a specific group of people/organizations by sending emails to gain access to what they need?

What to watch out for

- Congratulatory or warning emails from unknown senders
- An email with a call-to-action to "click here for a prize/cashback/points"
- A mismatch in the sender's email address vis-à-vis the official email address
- Emails addressing you with a generic title such as "valued customer" instead of your name
- Emails appearing to be from executive leadership you work with, requesting information about you or colleagues that they usually do not ask for
- Unexpected emails asking for your personal information or your immediate action

How to avoid falling prey to it

- Do not click on links or open attachments from unknown senders
- Do not respond to or forward suspicious emails that may be a scam
- Always make sure that the sender's email address matches the official address
- If in doubt, contact the person or organization (as claimed in the email) by using contact information provided only on their official website
- Always hover your mouse over the link to see if it will direct you to a legitimate website
- Do not enter any personal, login, or financial information when prompted by an unsolicited email

VISHING

Vishing (voice or VoIP phishing) is an electronic fraud tactic that can be conducted by voice email, VoIP (voice over IP), landline or cellular telephone. Vishing is the telephone equivalent of phishing, where fraudsters trick the user into divulging sensitive data by pretending to be someone else ***over a phone call.*** This private information can be used for identity theft.

What to watch out for

- A caller exhibiting over-friendly behavior (calling you by your first name or making small talk to get to know you)
- A caller who claims to work for a company or organization you trust (such as a bank, a software vendor, police department, or government agency)
- Threatening calls reiterating a fine or charge that must be paid immediately
- Calls claiming to distribute exaggerated/fake prizes, products, or services such as credit and loans, extended car warranties, charitable causes, or computer support
- A phone call requesting for login credentials or personal sensitive information, or suggesting you make a payment using odd methods, like gift cards
- Pre-recorded phone call messages or robo calls

How to avoid falling prey to it

- Never share sensitive information over a phone call
- Be suspicious of all unknown callers
- Always cross question the caller if you have any doubts

Smishing

Smishing stands for "SMS phishing," a security attack in which the user is tricked into downloading a Trojan horse, virus or other malware onto his cellular phone or other mobile device. This can also include fraudulent ***messages sent over on SMS*** to the trick user into divulging sensitive information.

What to watch out for

- Suspicious messages from unknown senders
- Impersonations of a business such as your bank or mobile service provider who try to convince you to respond to the message with information or ask you to click a link to log into your account or provide requested information, indicating a problem with your account and immediate action
- Text or SMS claiming you have won a prize or enticing you to click a link or send information to be entered to win something

How to avoid falling prey to it

- Do not call back on a phone number provided in any suspicious SMS
- Do not trust a sender just because their sender name is an abbreviated form of an assumed word, e.g. ICBNK
- Avoid clicking on any URL in the SMS
- Avoid downloading any app from a link mentioned in a suspicious SMS

Protecting your Information

- Mobile security tips
    - Research and download apps from a safe, trusted source.
    - Read the terms and conditions around app permissions before clicking on “I agree”.
    - Review the app ratings before deciding whether the content is appropriate for download.
    - Ensure your apps are updated regularly and watch out for new updates or permissions that the app may require.
    - If you are using a banking app or any other app for financial transactions, follow basic tips such as protecting your phone with a password, not changing factory security settings and/or logging out from the app when finished.
    - Use antivirus to keep you mobile device safe.

- Computer security and safe browsing tips
    - Be careful while clicking on any attachment or links in an email.
    - Beware of updating/uploading sensitive information on websites such as banking websites
    - Ensure your network connections are secure and you browse only on secure networks and not on a public network.
    - Create hard-to-guess passwords that include upper and lower case letters, numbers and special symbols.
    - When shopping online, or visiting websites for online banking or other sensitive transactions, ensure the site’s address starts with “https”, instead of just “http”, and has a padlock icon in the URL field.
    - Equip your computer with an updated anti-virus software.
    - Ensure your computer and mobile device have the latest software versions installed.
    - Change your password every 2 months.
    - Do not share your sensitive data as that may lead to identity theft.
    - Do not re-use your office computer password for personal emails and services.

NOTE: TransUnion CIBIL does not have any official mobile app. Please be wary of any such apps on the Android PlayStore or iOS App Store.