certin Handling Computer Security Incidents
Indian Computer Emergency Response Team
Ministry of Electronics and Information Technology
Government of India
सत्यमेव जयते

CERT-In Advisory CIAD-2017-0011

Safeguarding Online Identity

Original Issue Date: February 10, 2017

Description

The Digital India programme is a flagship programme of the Government of India with a vision to transform India into a digitally empowered society and knowledge economy. "Faceless, Paperless, Cashless" is one of professed role of Digital India.Securing the online transaction is a responsibility shared by each participant of digital payment systems. While the presence of user over web, theyestablish an online identity in online communities and websites, which in turn is used to share the information and make transaction in virtual world.

In the case of identity theft, this can be misused for making fraudulent transactions, availing benefits of the govt. schemes, to commit a another crime with the same identity and many more.

This document attempts to prevent and protect an innocuous user against online threats with the belief that online safety and security falls majorly under the domain of personal control and responsible online behavior. Owning identity in virtual world is an essential component of Responsible online behavior and advisory on this will enable users to contribute to build a more robust and resilient secure digital payment eco-system.

Incidents of identity theft

Identity theft happens when users fall for phishing, download malware, use insecure wireless networks, take out money from an ATM with a skimming device, falls for e-commerce skimming, share their passwords with people, or by having their personal information stolen by any means.

Following could be possible clues of identity theft

- Withdrawals from bank account without knowledge of user
- Disconnect in billing or email notifications
- Merchants refuse your cards/wallets
- E-Wallet balance exhausted
- Unfamiliar accounts or charges on your credit card

You get notice that your information was compromised by a data breach at a bank/e-wallet company where you have given your information

Best Practices for users

- Ensure that you have your strong passwords for all accounts. Use of non-dictionary words is also advised. Do not share your password with others.
- Shop with companies/websites you know. If the company is unfamiliar, investigate their authenticity and credibility. Conduct an internet search for the company/website name.
- Websites having click and wrap agreements, privacy policies, by reading these policies one knows about the uses of information by websites. Websites do sell this information. Some major social networking sites actually use or sell information (not personal data) about you to display advertising or other information they believe might be useful to you. Therefore it is advised that one should read the privacy policies of websites before getting into it.
- Minimum amount of information should only be disclosed such as screen name should not give a clue to the identity of the user.
- Avoid posting personal information such as your address, phone numbers, e-mail address, license number, Aadhar No, birth date, birth place, location for any given day, school's name of kids, and family details.
- While posting photos, avoid providing details of where you live, work or go to college. Also, do not post photos depicting negative or inappropriate behaviors, remember you are writing your own history and it will continue to exist in the cyber world.
- Look for encryption, before making any sort of digital payment, look for signs that show whether the website is encrypted or not. To do this, look for two things: the trusted security lock symbols and the extra "s" at the end of http in the URL or web address bar.
- Avoid connecting strangers since you don't know that your information could be used in a way you didn't intend.
- Verify emails and links in emails you supposedly get from your social networking site. These are often designed to gain access to your user name, password, and ultimately your personal information. These mails could be phishing emails too.
- Keep your anti-virus and software updated.
- Own your online identity - Check privacy and security settings and set it to your comfort level for information sharing
- Secure your login - Use strongest authentication tools wherever available and applicable, such as biometrics, security keys or a unique one-time code through an app on your mobile device. Your usernames and passwords are always not enough to protect key accounts like email, banking and e-wallets.

In cases of identity theft

- Ensure that you have changed your passwords for all accounts.Contact your banks/wallets to freeze your accounts so that the offender is not able to access your financial resources.
- Get your cards blocked and find out that if there have been any unauthorized transactions. Close accounts so that future charges are denied. Inform banks/wallets in through their grievance Redressal mechanism or customer care cell in writing too.

- Approach local law enforcement agency for reporting of fraud in addition to banks/wallets.
- If your personal information has been stolen through a banks/e-wallets/intermediaries data breach (when a offender hacks into a database of accounts to steal information), you will likely be contacted by the banks/e-wallets/intermediaries whose data was compromised with additional instructions, as appropriate. You may also contact the respective organization's grievance officer for more information.

References

http://www.idtheftcenter.org/
https://staysafeonline.org

Disclaimer

The information provided herein is on "as is" basis, without warranty of any kind.

Contact Information

Email: info@cert-in.org.in
Phone: +91-11-24368572

Postal address

Indian Computer Emergency Response Team (CERT-In)
Ministry of Electronics and Information Technology
Government of India
Electronics Niketan
6, CGO Complex, Lodhi Road,
New Delhi - 110 003
India