भारतीय बीमा विनियामक और विकास प्राधिकरण
INSURANCE REGULATORY AND DEVELOPMENT AUTHORITY OF INDIA
Promoting insurance. Protecting insured.

CYBER SECURITY AWARENESS CAMPAIGN
Oct-2021

Considering the increase in Information and communication technology penetration as well as digital activity especially during the Covid Pandemic, awareness about the Cyber security for policyholders and the general public is the need of the hour to prevent cyber frauds and crimes.

Here are a few Dos and Don'ts while carrying out various insurance transactions:

1.Buying/Renewing a Policy

Do's

- ☑ Look for credibility of sellers, namely agents, intermediaries such as brokers or insurance company staff
- ☑ Provide personal information only on need-to-know basis
- ☑ Provide KYC information when needed
- ☑ Use a **Strong password** to setup account in the insurance company's websites or web-aggregators if required

Don'ts

- ☒ Avoid insurance related websites NOT starting with *https*
- ☒ Avoid sellers/intermediaries with suspicious and spurious identity
- ☒ Beware of the insurance intermediaries' asking for sensitive information

2. Operating insurance Policy and communications

Do's

- ☑ Use strong passwords in the insurance accounts and login at insurance company portals
- ☑ Use impersonal and different passwords for different accounts
- ☑ Use genuine operating systems (on which operating using electronic insurance account)
- ☑ Keep your account password confidential
- ☑ Inform about any change in contact details, address to the insurance company from time to time

Don'ts

- ☒ DO NOT use default passwords
- ☒ DO NOT share any Pin/account password upon contacting Customer care service
- ☒ DO NOT share any OTP unless certain of its use

3. Claim process safety

Do's

- ☑ Provide authentic claim related information and personal/sensitive information as needed
- ☑ Provide genuine identification and KYC validations

Don'ts

- ☒ Provide account information only to insurance company's staff/claim team upon satisfaction of their authenticity
- ☒ Do NOT provide account passwords to anyone
- ☒ Keep records of the transaction's important information e.g. *transaction ID*

4. Protection from Phishing and suspicious communications

Do's

- ☑ Check for unfamiliar or illegitimate address
- ☑ Beware of 'sense of urgency' in the emails. Phishing e-mails have tendency to make the target feel rushed.
- ☑ Check for generic greetings/salutation in the doubtful e-mails e.g. *Dear Valued customer, Dear user* instead of name
- ☑ Try to identify phishing emails through spelling and grammatical mistakes in the mail content

Don'ts

- ☒ Never respond to requests for personal information via email
- ☒ Never enter personal information in a pop-up screen
- ☒ DO NOT click any links listed in e-mail. if the link is to be verified, copy and paste URL into browser.
- ☒ DO NOT click any suspicious attachments e.g. those containing *.exe file extensions*

5. Cyber Ethics - Be a responsible Cyber policyholder

- Do not engage in inappropriate cyber conduct, e.g. cyber bullying
- Do not impersonate anyone, e.g. by creating social pages, posts, sites etc.
- Adhere copyright constraints when downloading insurance or any other information from internet
- Do not use others' information which may identify them
- Use public Wi-Fi with care and caution

6. Reporting Cyber Crimes

1. **Helpline 155260 –** National Helpline and reporting platform by Ministry of Home Affairs (MHA)
    - Helps in preventing financial loss
    - Operated by concerned State Police
    - Uses new-age technologies to take action against digital fraud in real-time
    - Integration response with Law Enforcement Agencies and Financial Intermediaries
    - More information: https://cybercrime.gov.in/Webform/Helpline.aspx
2. https://digitalpolice.gov.in/Default.aspx: This portal is a platform for Citizens to file crime related complaints online and seek antecedent verification of prospective employees (including for domestic help, drivers etc.), tenants or for any other purpose. Citizens can also seek certification of their own antecedents.

A Public awareness initiative by IRDAI