Watch out! Fraud SMSes and calls are soaring

Awareness is key to ensuring you don't lose money, data

Swati.Bharadwaj@timesgroup.com

"Dear HDFC Customer your HDFC NET BANKING will be suspended today please update your PAN card now visit below the link…"

"Dear consumer your electricity power disconnect today 9:30 PM contact now! Billing officer…..because bill not update Thanks…"

Is your phone inbox swamped with such SMSes, exhorting you to share personal details or act urgently on some perceived threat? Are you inundated with rude callers threatening to block your credit or debit card, disconnect your mobile number or electricity connection unless you share sensitive data such as password, PAN, Aadhaar, OTP or CVV with them?

Many will recognise these to be frauds. But many will also get worried and do precisely what the fraudsters want them to. In the post-Covid world, the incidence of cybercrime has risen exponentially. While organisations, governmental and business, are the major targets, individuals too are increasingly being targeted, but data on that is limited.

HOW TO PROTECT AGAINST CYBERCRIME

- Never click on links sent on SMS or email from untrusted or suspicious senders
- Never share your personal information such as PAN card no., Aadhaar no., bank account no., credit or debit card no., PIN, CVV or OTP
- Use strong passwords which are a combination of upper and lowercase letters, special characters and numbers
- Keep your software & operating systems updated
- Use anti-virus software and regularly update security patches
- Contact banks or companies directly about suspicious requests
- Be careful about website URLs you are visiting
- Keep an eye on bank and credit card statements

Source: BlueVoyant, Vidhikarya & Kaspersky

EXPONENTIAL RISE IN CRIMES

"Not much research goes into retail fraud as it is too small to cover, and is least preventable because it involves a variety of customers that are exploited by fraudsters using human emotions such as greed and anxiety, and even factors such as ignorance," points out Sivarama Krishnan, partner & Apac cybersecurity leader in PwC India.

Krishnan says the only way to contain these frauds is through building awareness among individuals.

Abhyuday Data, director analyst - identity & access management division at Gartner, says that while the incidence of social engineering attacks is reducing, other forms of attacks like man-in-the-middle (MITM), distributed denial of service (DDoS), and multi-factor authentication (MFA) prompt bombing are increasing.

In an MITM attack, the hacker tricks the victim into disclosing sensitive information on call or via messages, or uses EvilProxy, which offers a cookie injecting mechanism, to get access to your OTP. An MFA prompt bombing is an effort to break your MFA protection – the hacker makes repeated attempts to log in your user name and password to tempt you to tap the notification link and gain access to your account.

According to Data, many organisations, especially banks, are now implementing transaction-based authentication, but they can reduce the incidence of phishing threats by migrating to phishing resistant authentication methods like FIDO2, which is a password-less authentication open standard that uses public-key cryptography for security and convenience, and ITDR that encompasses threat intelligence, practices, knowledge base, tools and processes to protect identity systems.

A recent Gartner report says that conventional identity and access management and security preventive controls are insufficient to protect identity systems from attack.

"Modern identity threats can subvert traditional identity and access management (IAM) preventive controls such as multi-factor authentication (MFA) which makes identity threat detection and response (ITDR) a top cybersecurity priority for 2022 and beyond," says the report.

KV Karthik, partner - financial advisory in Deloitte India, says that with fraud schemes and the sophistication of fraud perpetrators constantly evolving, analytical tools provide the ability to discern anomalies, patterns, and trends – across available data that might otherwise go unnoticed.

Players such as Quick Heal are leveraging deep learning, behavioural analysis and predictive analytics to come up with solutions that not only monitor systems to identify cyber attacks and analyse the severity of the threat, but also block such threats.

Krishnan of PwC points out that though an increasing number of cybercrime cases are coming to light in India, the numbers are much smaller for India compared to many other parts of the world. The total amount of fraud in India is less than 1% of the total transaction volumes, as compared to 2-4% globally. "So, while the individual affected may feel the pain, the overall percentage is not too alarming," he said, attributing it to the proactive approach of the Reserve Bank of India.

"What RBI has done with two-factor authentication and messaging back transaction alerts to consumers is unique," Krishnan says.