BBK

بنك البحرين والكويت

Best Practices and Recommendations: Debit Card users

- Memorize your PIN. Do not write it down anywhere. Do not disclose your ATM PIN details to anyone.
- Block the view of the number pad, so that nobody can notice your PIN. Never allow anyone to stand near you or help you complete transactions while at an ATM.
- If you get a transaction slip, tear it into pieces immediately after use if not needed.
- Remember to take your card and cash with you.
- Do not conduct any transaction if you find any unusual/suspicious device connected to your ATM. Please report the same to the Bank.
- Change your ATM PIN number regularly. Do not keep birthdays, anniversaries as PINs.
- While doing transactions at merchant establishment (POS), keep eyes on person swiping the card, if merchant asks for PIN, do not give it away. If PIN is required to be fed, please enter the PIN yourself.
- Erase the CVV number on backside of the card and memorize the same or store it confidentially.
- While doing ATM transactions if card is stuck in the machine, then do not get help if any stranger offers to do so. Cash retraction facility has been withdrawn.
- If your ATM card is lost or stolen, report the same to Bank branch, alternately you can block your card on your Mobile Banking app immediately. Please avail mobile banking facility to activate this service 24 * 7. If you have any complaint about your ATM/Debit/Credit Card transaction at an ATM, please take it up with your Card-issuing branch.

******End******

Best Practices and Recommendations: Android Mobile app users

- Reduce the risk of downloading potentially harmful apps by limiting your download sources to official app stores, such as your device's manufacturer or operating system app store.
- Prior to downloading / installing apps on android devices (even from Google Play Store):
- Always review the app details, number of downloads, user reviews, comments and "ADDITIONAL INFORMATION" section.
- Verify app permissions and grant only those permissions, which have relevant context for the app's purpose.
- Do not check "Untrusted Sources" checkbox to install side loaded apps.
- Install Android updates and patches as and when available from Android device vendors.
- Do not browse un-trusted websites or follow un-trusted links and exercise caution while clicking on the link provided in any unsolicited emails and SMSs.
- Install and maintain updated anti-virus and antispyware software.
- Look for suspicious numbers that don't look like real mobile phone numbers. Scammers often mask their identity by using email-to-text services to avoid revealing their actual phone number. Genuine SMS messages received from banks usually contain sender id (consisting of bank's short name) instead of a phone number in sender information field.
- Do extensive research before clicking on link provided in the message. There are many websites that allow anyone to run search based on a phone number and see any relatable information about whether or not a number is legit.
- Only click on URLs that clearly indicate the website domain. When in doubt, users can search for the organization's website directly using search engines to ensure that the websites they visited are legitimate.
- Consider using Safe Browsing tools, filtering tools (antivirus and content-based filtering) in your antivirus, firewall, and filtering services.
- Exercise caution towards shortened URLs, such as those involving bit.ly and tinyurl. Users are advised to hover their cursors over the shortened URLs (if possible) to see the full website domain, which they are visiting or use a URL checker that will allow the user to enter a short URL and view the full URL. Users can also use the shortening service preview feature to see a preview of the full URL.
- Look out for valid encryption certificates by checking for the green lock in the browser's address bar, before providing any sensitive information such as personal particulars or account login details.
- You should report any unusual activity in your account immediately to your branch with the relevant details for taking further appropriate actions.

******End******

BBK

بنك البحرين والكويت

Cybersecurity Awareness Campaign: Phishing

This is an awareness campaign regarding phishing attempts, as detailed below.

What is Phishing?

Phishing is a way of attempting to acquire information such as usernames, passwords, PIN, bank account, credit card details by masquerading as a trustworthy entity details through electronic communication means like e-mail.

Phishing is typically carried out by e-mail spoofing or instant messaging, and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one. Phishing is an example of social engineering techniques used to deceive users.

If something seems fishy...it's probably phishing. Here are some tips to keep in mind to avoid falling victim so that we protect our Bank and its data:

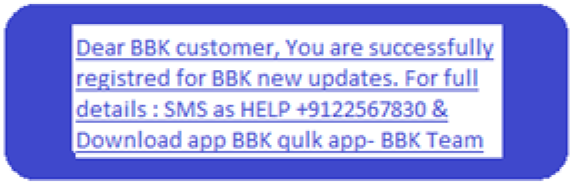
- Double-check that the sender's email address matches who they claim to be
- Don't click a link or download from emails sent by someone you don't know, or weren't expecting
- Typically, these emails will be poorly drafted with spelling mistakes. This should serve as an alert.
- Don't reply to a suspicious email or message from an email you don't recognize

******End******

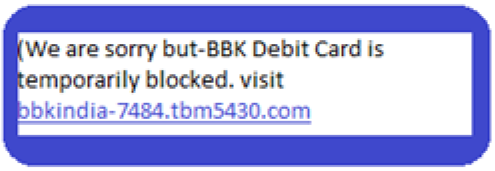
Cybersecurity Awareness Campaign: Smishing

Smishing uses cell phone text messages to lure users in a similar fashion like Phishing. They take the form of text messages that claim to be from legitimate entities and are often used in combination with other techniques to bypass inbuilt protections. They might also direct victims to malicious websites on their phones.

Typical Examples of Smishing Attacks



Dear BBK customer, You are successfully registred for BBK new updates. For full details : SMS as HELP +9122567830 & Download app BBK qulk app- BBK Team

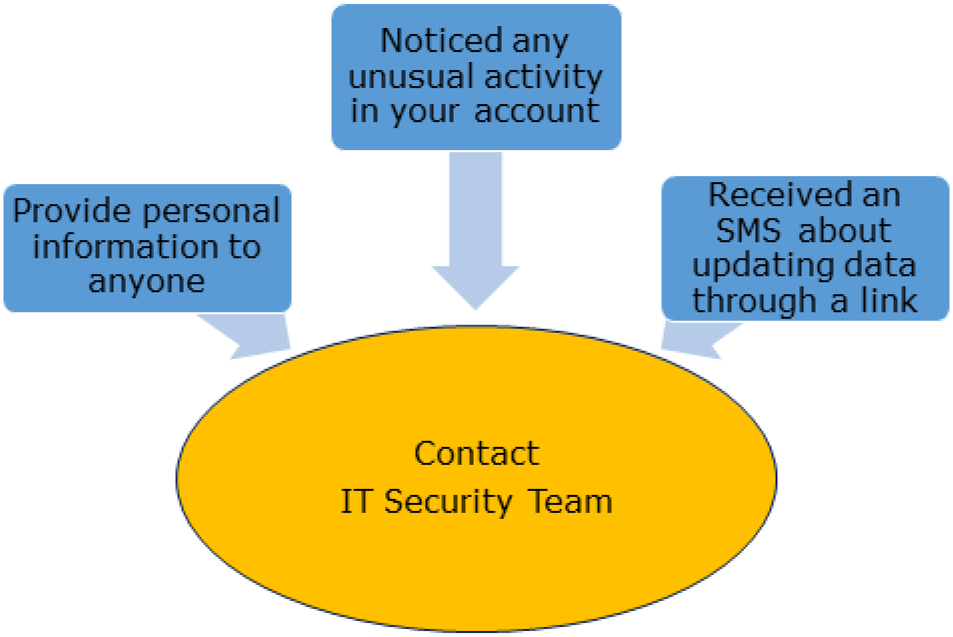


(We are sorry but-BBK Debit Card is temporarily blocked. visit bbkindia-7484.tbm5430.com

Best practices to follow to avoid Smishing attacks:

- Be suspicious of any text messages containing urgent request for personal or financial information.
- Do not share any sensitive information over text messages.
- Do not click on any links on the SMS.
- Please call the branch for help or refer to the information only on the official website of the bank.

Get in touch with your branch if you have



Noticed any unusual activity in your account

Provide personal information to anyone

Received an SMS about updating data through a link

Contact IT Security Team

******End******

Cybersecurity Awareness Campaign: Malicious APK files

Cyber criminals are using techniques to harvest user credentials, steal OTP etc. There have been several instances of cyber fraudsters using malicious Android Applications sent through SMS and Email. Multiple social engineering techniques in the name of cashback, KYC etc. are used to lure victims download the malicious mobile application. Same application is used with several banking customers by changing logo/ file/ bank name.

Modus Operandi:

- Fraudsters sends link to malicious APK file using bulk SMS to potential victims.
- Victim clicks on the short link which results in malicious APK getting downloaded on his/ her mobile
- Permissions are exploited by Android Application for stealing OTP and phone information including Send, Receive, Read, Write and Broadcast SMS.

Recommendations:

- To minimize the chances of falling victim to phishing attacks of this kind, only download Android apps from the official Google Play Store.
- Furthermore, always review the requested permissions carefully and do not install an app that is asking for greater privileges than it should require for its functionality.
- Finally, keep your device up to date by applying the latest available security updates and using a mobile security solution from a reputable vendor.

******End******

Cybersecurity Awareness Campaign: Password Security

Passwords should be unique from previously used passwords. Use different passwords for each of your important accounts, like your email and online banking. Reusing passwords for important accounts is risky. If someone gets your password for one account, they could access your email, address, and even your money.

Passwords should be created so that they can be easily remembered. For e.g., if you are a movie buff while you might think it's fun to use your favourite English movie as a password, it can actually be quite risky. You can start using vernacular movie name as passwords instead. E.g., sholaaurshabnam, Meevasantrao, Paranjaijaliyare, Thenmavinkombathu (all are vernacular movies, easy to remember for Hindi, Marathi, Bengali and Malayalam speaking citizens however very difficult to crack)

PASSWORD SECURITY, A SHORT STORY...
I JUST FINISHED UPLOADING ALL MY RESEARCH TO MY NEW SECURE SERVER. YOU'LL NEVER GUESS THE PASSWORD!
WATSON!
YOUR DOG'S NAME IS WATSON? RIGHT?
I'LL BE RIGHT BACK.
I ♥ My Dog

******End******

BBK
بنك البحرين والكويت

Cybersecurity Awareness Campaign: Strong Password

One of the ways to protect yourself and BBK from cyber threats is by having a strong password.
It's simple – the longer and more complex your password, the more difficult it is to crack. Shorter and simpler passwords take less time and resources for hackers to compromise.

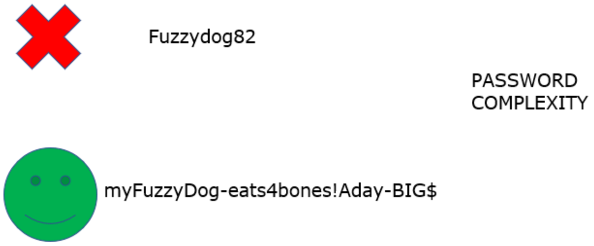
Traits of a Bad Password

Hackers have created databases of the most common words, phrases, and number combinations that they can run your password through to find a match. The following are some common password themes that you should avoid:

Birthdays;
Names;
Phone numbers;
Sports teams;
BBK information;
and Simple obfuscation of a common word ("P@$$w0rd").

What Makes a Good Password?

Your password should be at least 8 characters long, with at least one capital letter, one number, and one special character ("@", or "%", etc.).As an added layer of security, change your passwords on a regular basis to ensure that you stay ahead of the hackers. Remember, the best passwords contain as much randomness as possible – using unlikely combinations and random characters is a great strategy. Be creative!



It's important to remember that you should not use the same password for multiple accounts – no matter how strong it is – because if one account gets compromised, then they're all compromised.

Thanks again for helping to keep our network and our people safe from cyber threats.

******End******

BBK
بنك البحرين والكويت

Cybersecurity Awareness Campaign: Ransomware Awareness

Here are some simple things you can do to help BBK avoid a ransomware/malware attack:

The most common way ransomware enters corporate networks is through email. Often, scammers will include malicious links or attachments in emails that look harmless. To avoid this trap, please observe the following email best practices:

* Do not click on links or attachments from senders that you do not recognize. Be especially wary of .zip or other compressed or executable file types.
* Do not provide sensitive personal information (like usernames and passwords) over email.
* Watch for email senders that use suspicious or misleading domain names.
* Be especially cautious when opening attachments or clicking links if you receive an email containing a warning banner indicating that it originated from an external source.

If Something Seems Wrong, Notify IT Security Team

If your computer is infected with ransomware, you will typically be locked out of all programs and a “ransom screen” will appear. Please notify IT Security Team immediately.

Thanks again for helping to keep our network and our people safe from these cyber threats.

******End******

Cybersecurity Awareness Campaign: Phishing Mail Attacks

Globally, email phishing attacks are commonly used as a starting point by cybercriminals to gain access into the network of targeted entities. In order to assess the preparedness of banks against such attacks, RBI recently conducted a phishing Simulation Exercise. During the exercise, the learnings identified are.

1. The targeted users clicked on the phishing link, highlighting that they were unable to identify, or they were unaware about “Domain Name Disguise” email spoofing attack. Moreover, a few users who have access to generic email IDs were also found to be vulnerable to phishing email attacks.
2. The understanding /awareness of the targeted users about the need to check legitimacy of website links before clicking on them was found deficient. Further, a few users also submitted credentials such as name, email id etc. on the spoofed (look-a-like) webpage(s).
3. Certain users forwarded the dummy phishing email to other users, thereby increasing the chances of materialisation of the threat.
4. Some users clicked the phishing link contained in repeat dummy phishing email sent to them, indicating that such emails sent earlier were probably ignored by users just by chance.

******End******