Building Intelligent Enterprises

“Safe Online Banking”

Presented By:

18th August 2017

D.S. Gokul Chandar

DGM & CISO

The Karur Vysya Bank Ltd

KVB

CII Confederation of Indian Industry CONNECT Coimbatore 2017

Access your Bank Accounts from a secure location

- It’s always best practice to connect to your Bank’s website using computers and networks you know and trust.
- Free WiFi networks are definitely not advisable.
- Do not use the computers used for normal browsing, for accessing online banking accounts.
- In Business locations, it is a good practice to separate the networks for accessing trusted and untrusted sites. Have strong Firewall and Proxy controls for the trusted network segment.

Avoid clicking through emails

- Do not click on web links to go to the Bank’s website.
- You might end up landing in fraudulent websites designed to capture your personal information.
- It is a good practice to directly enter the Bank’s website name in the address bar in your browser.
- Do not open any file attachment received from unknown sources.
- Never click on “Yes” for remembering credit card number / Password / CVV when prompted by any website.

CII
Confederation of Indian Industry
CONNECT
Coimbatore 2017

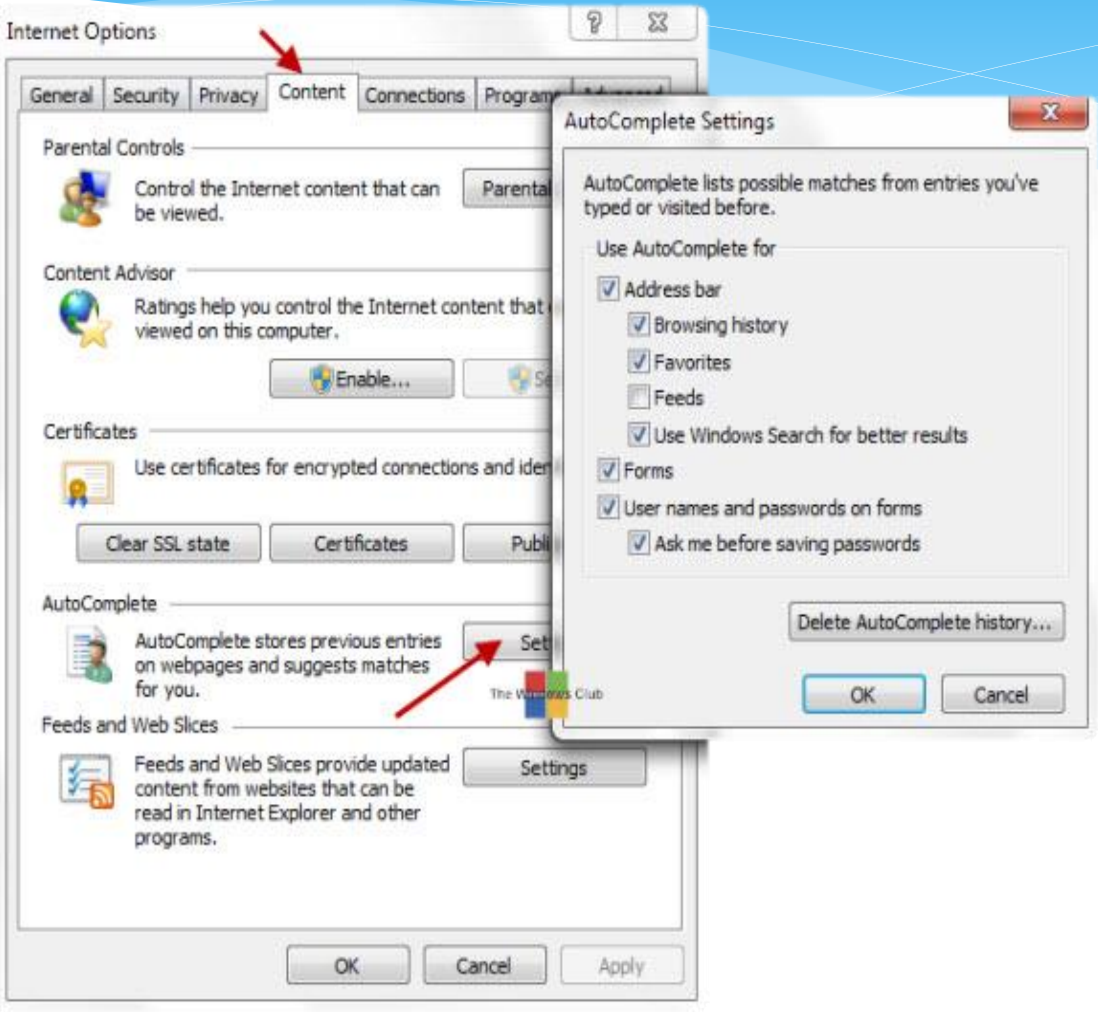
KVB

Secure your computer and keep it up-to-date

Ensure

- Antivirus is installed on Machine.
- Updated with latest patches (Antivirus & Operating System Security Patches).
- Full scan is performed periodically.
- Email Attachments and USB Devices are scanned before opening.

Disable the 'AutoComplete' function within your browser



Internet Options

Parental Controls

Control the Internet content that can be viewed.

Content Advisor

Ratings help you control the Internet content that viewed on this computer.

Certificates

Use certificates for encrypted connections and iden

AutoComplete

AutoComplete stores previous entries on webpages and suggests matches for you.

Feeds and Web Slices

Feeds and Web Slices provide updated content from websites that can be read in Internet Explorer and other programs.

AutoComplete Settings

AutoComplete lists possible matches from entries you've typed or visited before.

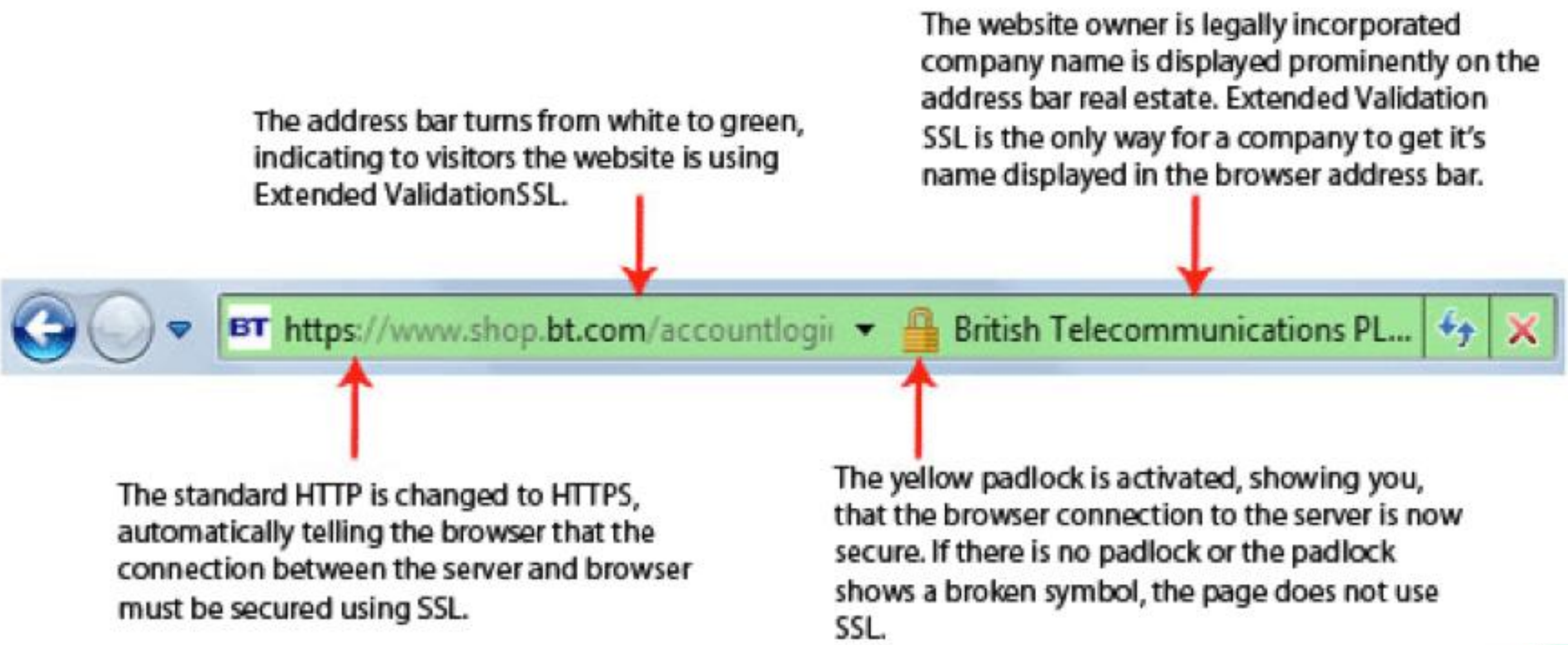
Use AutoComplete for

- ☑ Address bar
  - ☑ Browsing history
  - ☑ Favorites
  - □ Feeds
  - ☑ Use Windows Search for better results
- ☑ Forms
- ☑ User names and passwords on forms
  - ☑ Ask me before saving passwords

CII Confederation of Indian Industry CONNECT Coimbatore 2017

KVB

Validate the SSL Certificate



The address bar turns from white to green, indicating to visitors the website is using Extended ValidationSSL.

The website owner is legally incorporated company name is displayed prominently on the address bar real estate. Extended Validation SSL is the only way for a company to get it's name displayed in the browser address bar.

The standard HTTP is changed to HTTPS, automatically telling the browser that the connection between the server and browser must be secured using SSL.

The yellow padlock is activated, showing you, that the browser connection to the server is now secure. If there is no padlock or the padlock shows a broken symbol, the page does not use SSL.

BT
https://www.shop.bt.com/accountlogi
British Telecommunications PL...

Validate the SSL Certificate

- If you are in any doubt, click on the lock icon 🔒 on the right hand side in the address bar on the top of the page.
- Click on "View Certificate". This opens up a new window, displaying the SSL certificate information.
- Ensure that there is no red cross mark preceding the title 'Certificate Information'.
- Ensure that the Certificate is issued to your Bank, e.g. "kvb.co.in".
- Make sure that the certificate is currently valid.

Create a strong password

- When you **create** your **password**, make it at least 8 characters long.
- Include at least one capital letter, one numerals (0-9) and one special character (like @, #, $, etc).
- This makes the password very difficult to crack.
- It should be **Easy** to **remember** & **Difficult** to **Guess.**

Create a strong password

- **Change** the password **frequently** and never keep same password for all the accounts.

- When setting up online banking, if your bank asks you to provide answers to some standard **security questions** remember that the **answer you give doesn’t have to be the *real* one**.

Always log out when you are done

- It is good practice to always log out of your online banking session when you have finished your business and close the browser. This will lessen the chances of falling prey to **session hijacking and cross-site scripting exploits.**

- You may also want to set up the extra precaution of **private browsing on your computer or smart phone,** and set your browser to clear its cache at the end of each session.

Set up account notifications

- For **withdrawals** matching or exceeding a specified amount.
- If account balance dips below a certain threshold.
- For account balance on a **daily basis.**
- Setup both your mobile number and email ID for receiving such notifications.
- Setup two factor authentication for your emails.
- Do not ignore these alerts, they would give you quick notice of suspicious activity in your account.
- Be wary of alerts not received for genuine transactions done.

Controls for Corporates

- Ensure that online Banking profile is created exclusively for each authorised user/employee. Do not share user profiles.
- Ensure that access to the Bank's website is always protected by two factor authentication (i.e.: password and OTP/Token).
- Setup transaction limits/thresholds for each employee.
- Ensure that maker / checker control exists for each transaction.
- Additional authorisation can be configured for high value transactions

Monitor your accounts regularly

- Why wait for the month end to review the account statement and discover a discrepancy?
- With online banking you have **access 24/7** so take advantage and check your account on a regular basis.
- Look at every transaction since you last logged in. If you **spot any anomalies**, contact your **Bank immediately.**
- Corporates should **reconcile** their Bank accounts with their internal accounts daily.

Mobile Banking Security

- Install mobile security software in your device and keep it updated.
- Don't forget to install updates for your device operating system.
- Always secure your phone with a PIN / pattern / finger print.
- Download the Mobile Banking App only from trusted sources. Download App updates regularly as they include fixes to security flaws.
- Do not set your phone settings to auto-fill User ID's or Password information.
- Do not use Jail Broken / Rooted Device to access Mobile Banking App.
- Ensure device safety.

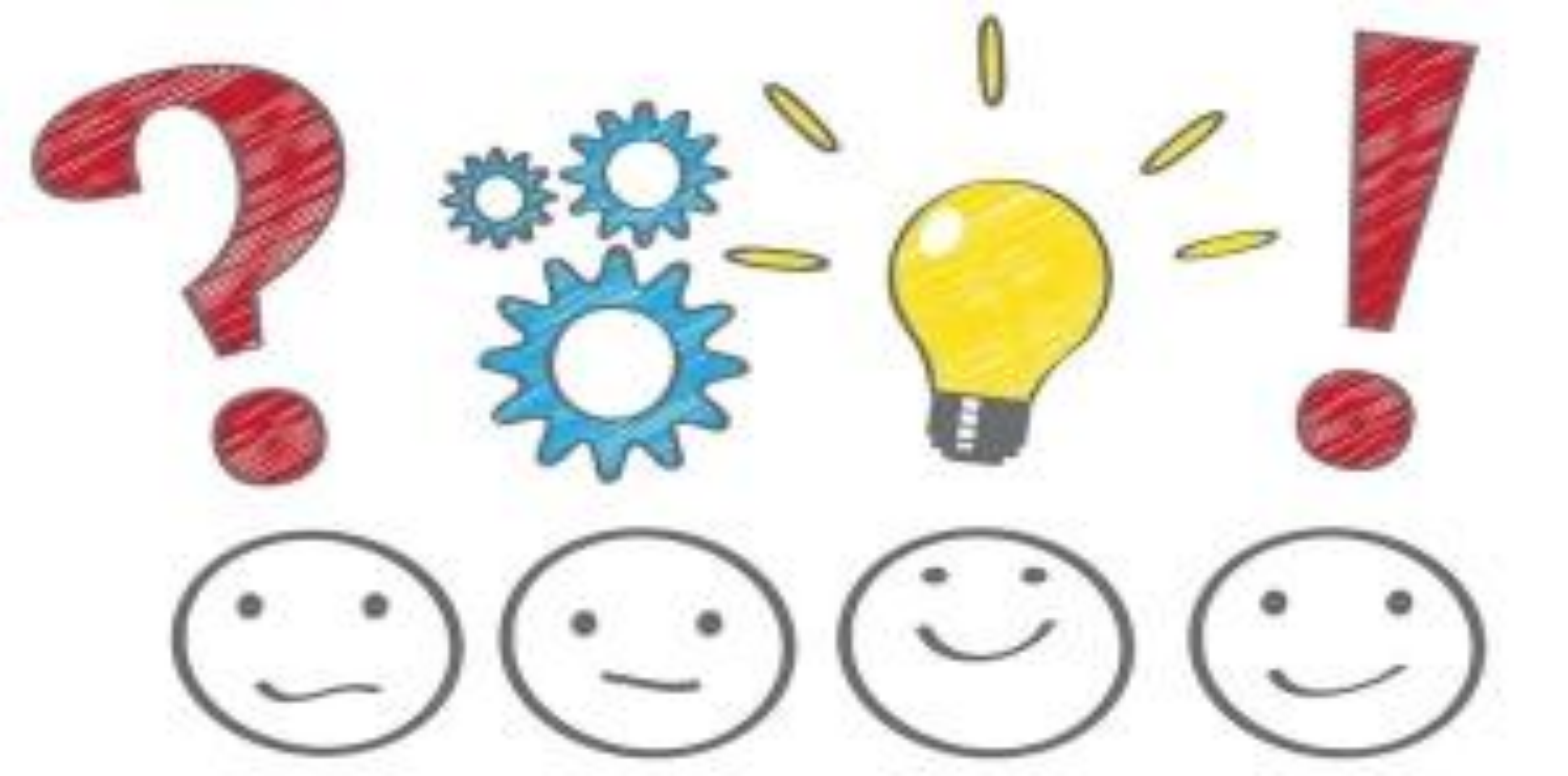
CII Confederation of Indian Industry CONNECT Coimbatore 2017

KVB

When in doubt, reach out to your Bank

- Your Bank will not send any requests asking you to disclose your **Passwords, Credit/Debit Card numbers, Bank account numbers, or other personal or financial information.**
- In case you get an email or a phone call asking your personal security details, reach out to your Bank for guidance.
- If any Bank staff approaches you to disclose your User ID / password, please report the matter to your Bank immediately.

Questions



Happy Banking ☺

Thank You