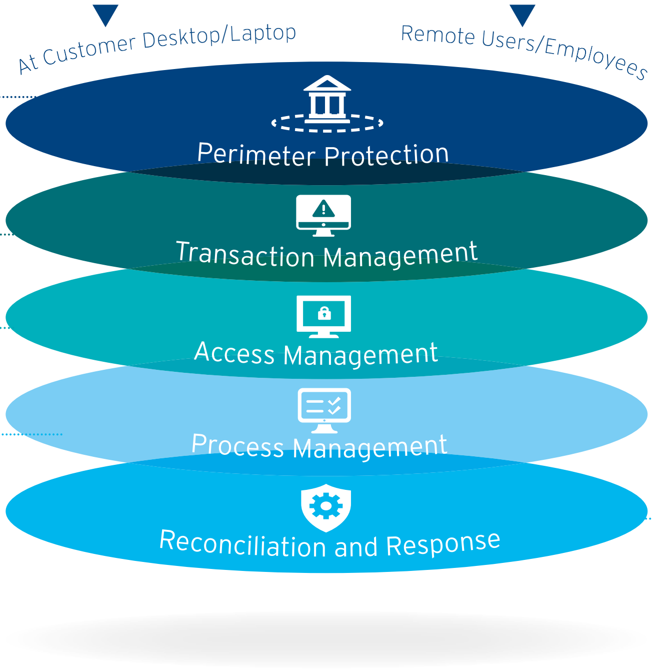
Treasury and Trade Solutions

citi®

Digital Security Best Practices for Online Banking and File Connectivity

The best defense is known as a ‘layered defense’ which should be created by utilizing best practices from the industry, financial market utilities and law enforcement

A layered defense checklist:



Perimeter Protection

- Ensure secure connectivity between third-parties with firewalls and encryption
- Restrict access to sensitive systems (e.g. online banking, Enterprise Resource Planning, and treasury management systems)
- Conduct vulnerability assessments to proactively identify and mitigate weaknesses
- Use anti-virus protection and anti-phishing tools by filtering emails and suspicious links

Transaction Management

- Restrict entitlements for high risk functions such as transaction initiations, beneficiary changes, business accounts, and confidential data within the organization
- Create authorization limits and segregation of duties for high value transactions (e.g. up to 9 levels of approvals on CitiDirect BE®)
- Set controls for the sharing and modification of files, messages, and other data (e.g. monitoring of data leaving your company)
- Be vigilant in reviewing transaction details prior to submission

Access Management

- Never leave an active session unattended
- Log out at the end of each CitiDirect BE® session
- Never share your login credentials or write down the PIN, especially on the back of physical tokens
- Use strong passwords or multi-factor authentication to protect business devices and applications

Process Management

- Create and promote training on fraud awareness and business procedures
- Regularly update your software and business devices (e.g. Operating system, browsers, Java, and Adobe Flash)
- Follow Citi Connectivity and Encryption standards when completing CitiConnect onboarding
- Ensure company policies are in place and followed for data retention, storage and privacy
- Rotate or require mandatory absence from staff in sensitive or financial assignments
- Report any suspicious activities to your Information Security team or Citi (e.g. Citi URL modification, phishing emails, social engineering calls claiming to be from a Citi source, etc.)

Reconciliation and Response

- Daily and intraday account reconciliation using multiple means
- Validate supplier information on a periodic basis
- Regularly review transaction reports and dashboards and conduct user audits
- Leverage internal fraud resources to monitor for suspect payments
- Issue alerts and reminders to staff on what they should do in the event of an actual or potential compromise
- Document transaction recall processes and conduct periodic tests of response

Treasury and Trade Solutions
transactionservices.citi.com

GRA27735 11/2016