Online Banking Fraud Prevention Recommendations and Best Practices

Continental National Bank

This document provides you with fraud prevention best practices that every employee at Continental National Bank of Miami needs to know in order to educate our Online Banking users.

User ID and Password Guidelines

Your Logo

User ID and Password Guidelines

1. Create a “strong” password with at least 8 characters that includes a combination of mixed case letters, numbers, and special characters “!@#$%^&*(){}<>”.

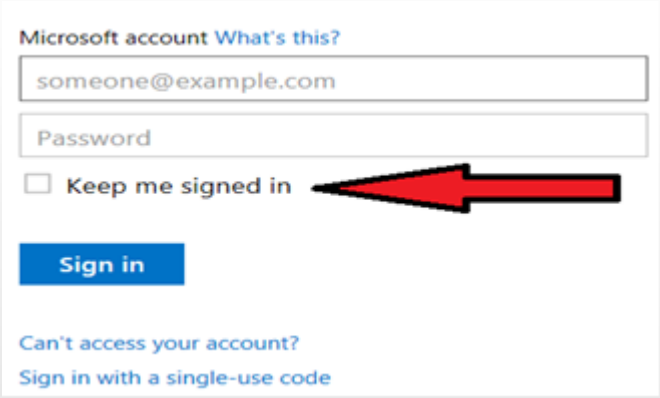
OK Password:	Better Password:	Excellent Password:
ilovemypiano	ILoveMyPiano	ILov3MyPi@no
ihateliverandonions	1Hateliver@ndonions	1Hat3liver@Onions!
mypuppylikescheese	MyPuppyLikesCh33s3	.MyPuppyLikesCh33s3
julieloveskevin	JulieLovesKevin	Jul1eLovesK3v1n
ieatcarrots	IeatCarrots	I34tcarr0ts:

2. Change your password frequently preferably each 60 days.

3. Never share username and password information with anybody.

4. Do not use account numbers, your social security number, or other personal information when create user name and password.

5. ***Avoid using an automatic login feature that saves usernames and passwords, such as the one below:***



Online Banking General Guidelines

Your Logo

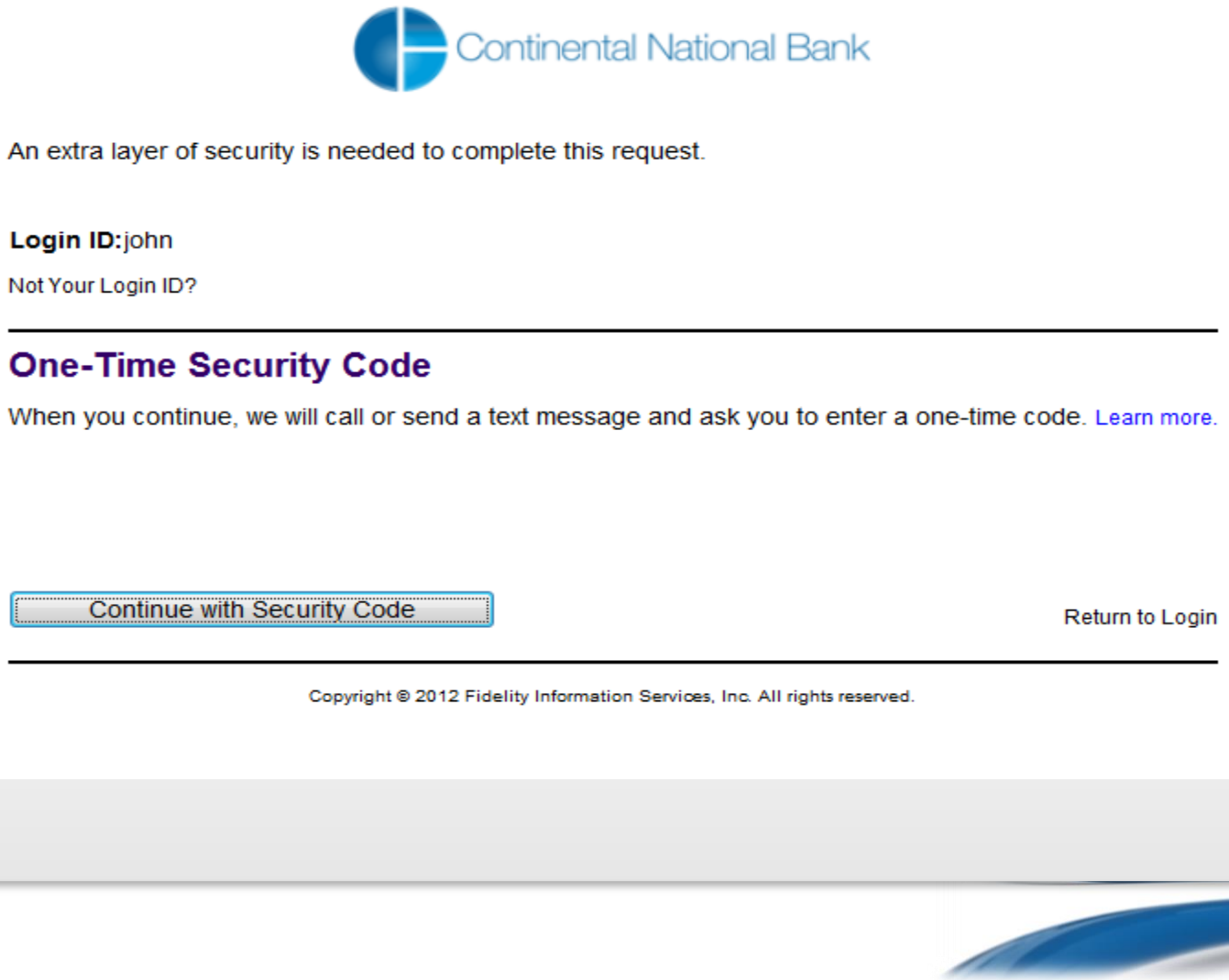
Online Banking General Guidelines

1. Do not use public or other unsecured computers for logging into Online Banking or for financial transactions (for example, one at a library or coffee shop).
2. Review account balances and detail transactions regularly (preferably daily) to confirm payment and other transaction data and immediately report any suspicious transactions to your financial institution.
3. View transfer history available through viewing account activity information.
4. Whenever possible, use Bill Pay instead of checks to limit account number dissemination exposure and to obtain better electronic record keeping
5. **Do not use account numbers, your social security number**, **or other account or personal** information when creating account nicknames or other titles.
6. Review historical reporting features of your online banking application on a regular basis to confirm payment and other transaction data.
7. **Never leave a computer unattended while using Online Banking.**
8. Never conduct banking transactions while multiple browsers are open on your computer.
9. **An FBI recommended best practice is to suggest that company users dedicate a PC solely for financial transactions (e.g., no web browsing, emails, or social media).**

Online Banking General Guidelines

10

Whenever possible, register the computer you use specifically for Online Banking in order to avoid having to re-send a security code and other authentication information with each login.

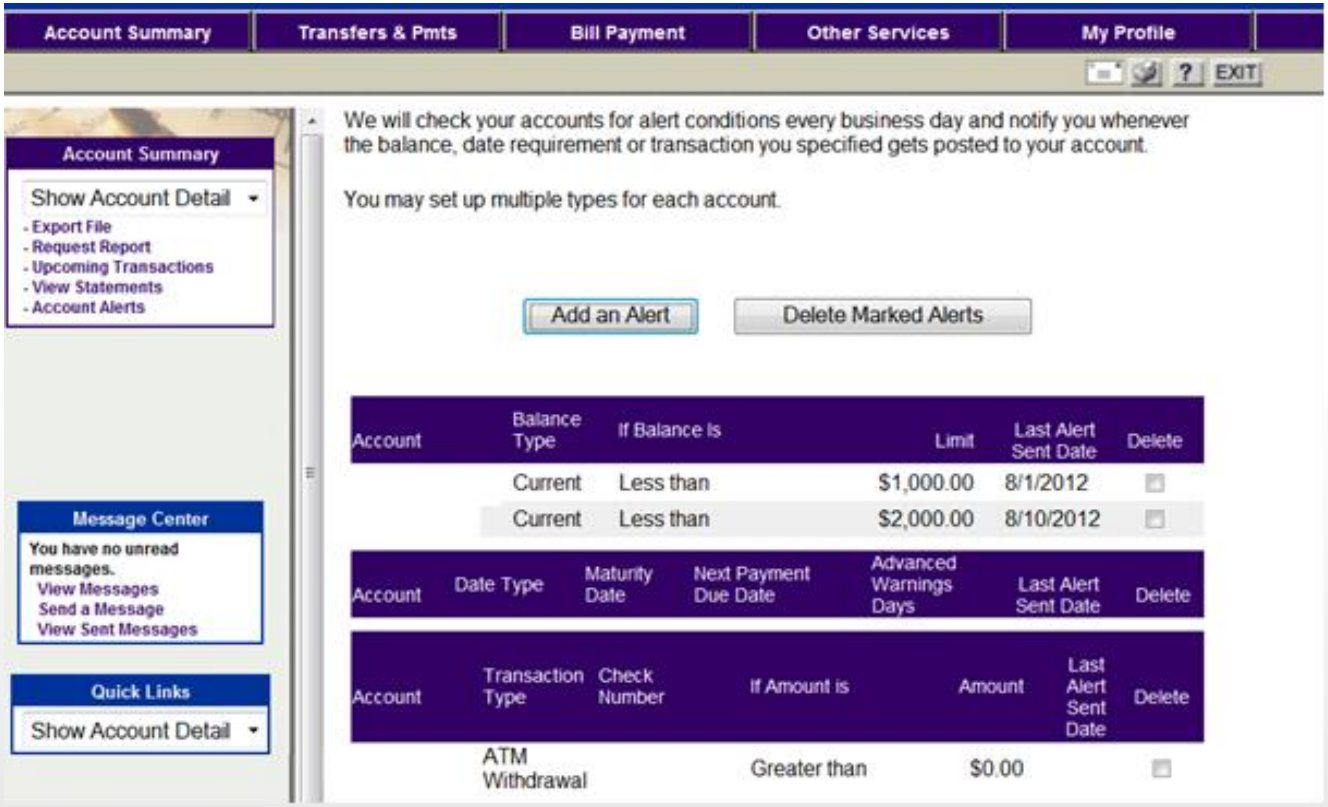


Online Banking General Guidelines

11

Take advantage of and regularly view system alerts; examples include:

- Balance alerts
- Transfer alerts
- Password change alerts
- ACH Alerts (for cash management users)
- Wire Alerts (for cash management users)

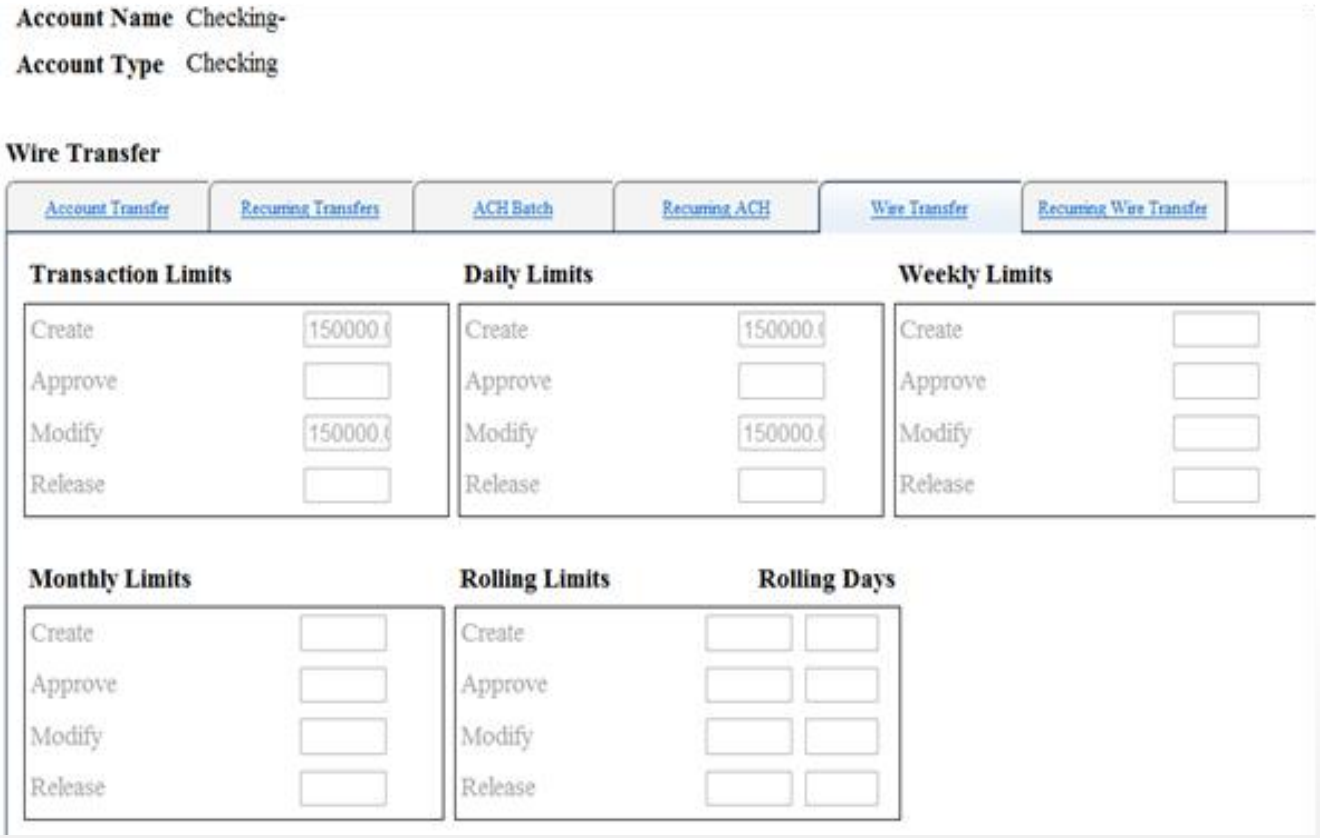


Tips to Protect Online Transfers, Payments & Account Data

Your Logo

Tips to Protect Online Transfers, Payments & Account Data

1. Take advantage of transaction limits. Establish limits for monetary transactions at multiple levels: per transaction, daily, weekly, or monthly limits. (for cash management users)



2. When you have completed a transaction, ensure you **log off** to close the connection with the financial organization's computer.

Tips to Avoid Phishing, Virus, Spyware and Malware

Your Logo

Tips to Avoid Phishing, Virus, Spyware and Malware

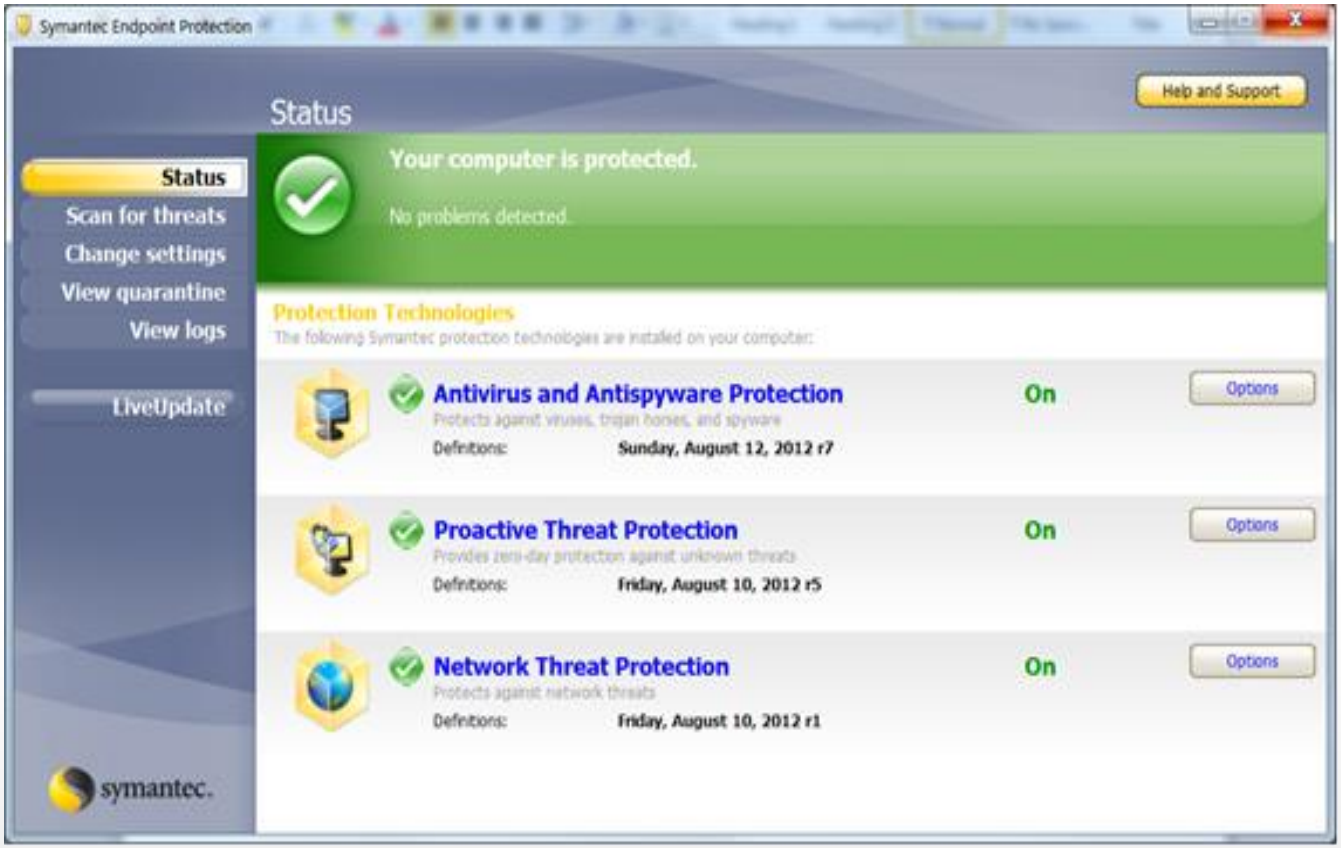
1. **Do not open e-mail from unknown sources.** Be suspicious of e-mails purporting to be from a financial institution, government department, or other agency requesting account information, account verification, or banking access credentials such as usernames, passwords, PIN codes, and similar information. Opening file attachments or clicking on web links in suspicious e-mails could expose your system to malicious code that could hijack your computer.

2. **Never respond to a suspicious e-mail or click on any hyperlink embedded in a suspicious e-mail**. Call the purported source if you are unsure who sent an e-mail

3. If an e-mail claiming to be from your financial organization seems suspicious, checking with your financial organization may be appropriate.

Tips to Avoid Phishing, Virus, Spyware and Malware

4 **Install anti-virus and spyware detection software on all computer systems. Free software may not provide protection against the latest threats compared with an industry standard product.**

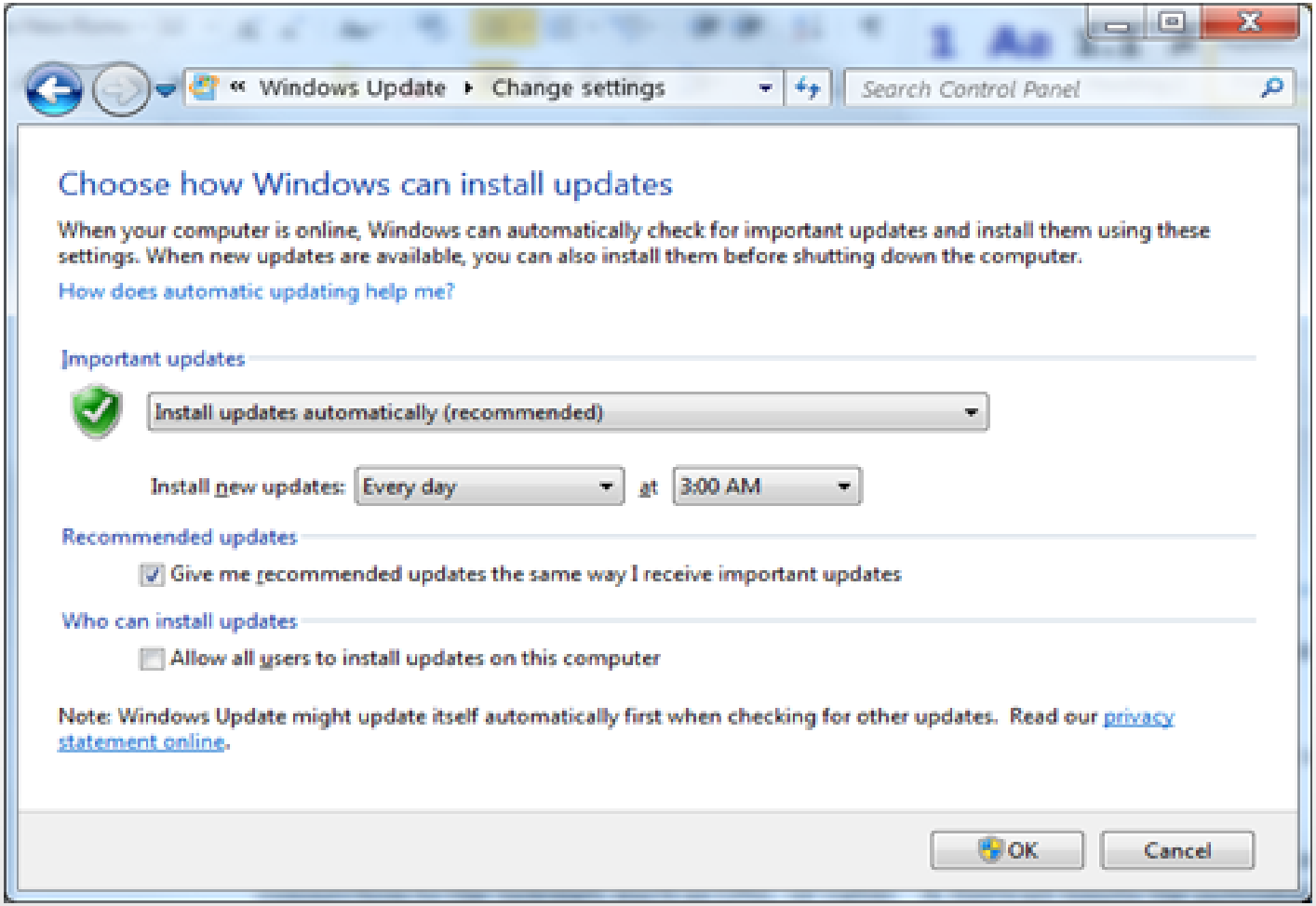


5 Update your computers regularly with the latest versions and patches of both anti-virus and anti-spyware software.

Tips to Avoid Phishing, Virus, Spyware and Malware

6

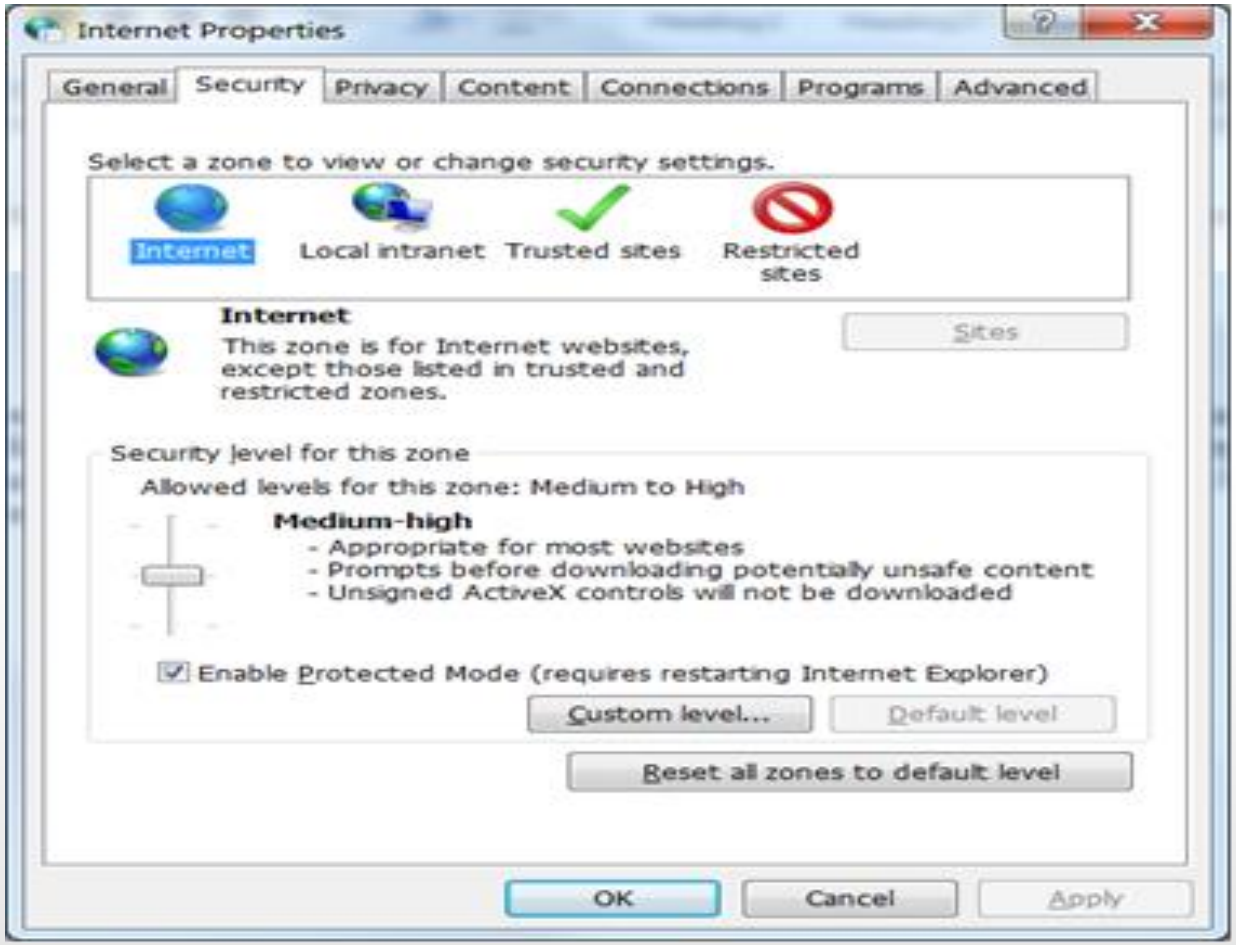
Ensure computers are patched regularly, particularly operating system and key application with security patches.



Tips to Avoid Phishing, Virus, Spyware and Malware

8 **Install a dedicated, actively managed firewall, especially if using a broadband or dedicated connection to the Internet, such as DSL or cable.** A firewall limits the potential for unauthorized access to your network and computers

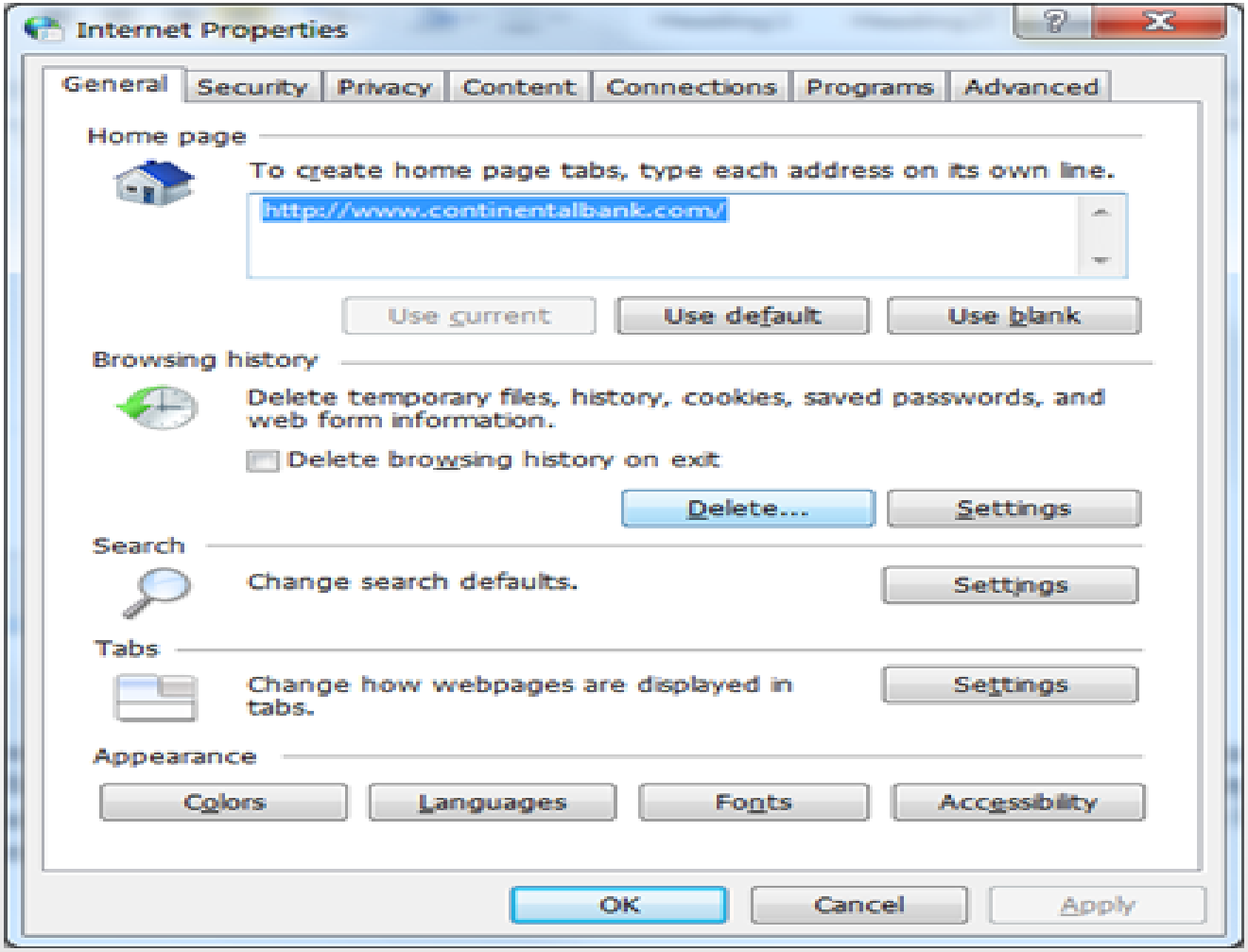
9 Check your settings and select, at least, **a medium level of security for your browsers.**



Tips to Avoid Phishing, Virus, Spyware and Malware

10

Clear the browser cache before starting an online banking session in order to eliminate copies of Web pages that have been stored on the hard drive. How the cache is cleared depends on the browser and version you are using.



Tips for Wireless Network Management

Your Logo

Tips for Wireless Network Management

Wireless networks can provide an unintended open door to your business network. Unless a valid reason exists for wireless network use, it is recommended that all wireless networks be disabled. If a wireless network is to be used for legitimate business purposes, it is recommended that wireless networks be secured as follows:

1. **Change the wireless network hardware (router /access point) administrative password from the factory default to a complex password.** Save the password in a secure location as it will be needed to make future changes to the device.
2. **Disable remote administration** of the wireless network hardware (router / access point).
3. If possible, **disable broadcasting the network SSID**.
4. If your device offers WPA encryption, **secure your wireless network by enabling WPA encryption of the wireless network**. **If your device does not support WPA encryption, enable WEP encryption.**
5. If only known computers will access the wireless network, consider enabling MAC filtering on the network hardware. Every computer network card is assigned a unique MAC address. MAC filtering will only allow computers with permitted MAC addresses access to the wireless network.

THANK YOU!