# Computer and Mobile Device Security Tips

Metropolitan Commercial Bank
The Entrepreneurial Bank

### We are all targets for hackers

We are at risk and the stakes are high to protect your personal and financial well-being from cyber-attacks. At Metropolitan Commercial Bank, we take cyber security seriously. We have measures in place to protect you and your accounts. In addition, by following the tips below and remaining vigilant, you are doing your part to protect you, your family and your business.

### Keep software up to date

Installing software updates for your operating system and programs is critical. Always install the latest security updates for your devices:

- Turn on automatic updates for your operating system.
- Use web browsers such as Apple Safari, Google Chrome, Microsoft Internet Explorer, Microsoft Edge or Mozilla Firefox or other browsers that receive frequent, automatic security updates.
- Make sure to keep browser plug-ins (Flash, Java, etc.) up to date.

### Avoid phishing scams – beware of suspicious emails and phone calls

- Phishing scams are a constant threat – using various ploys, cyber criminals will attempt to trick you into divulging personal information such as your login ID and password, banking or credit card information and more.
- Phishing scams can be carried out by phone, text or through social networking sites, but most commonly by email.
- Be suspicious of any official-looking email message or official-sounding phone call that asks for personal or financial information.

### Practice good password management

We all have too many passwords to manage – and it's easy to take short-cuts, like reusing the same password.

Here are some general password tips to keep in mind:

- Use long passwords. You can use easy to remember phrases, just make sure you use a mix of upper and lowercase letters, and numbers.
- Avoid using the same password for all of your logins.
- Don't share your passwords and don't write passwords down (especially not on a post-it note attached to your monitor).
- Update your passwords periodically, at least once every six months.

### Install anti-virus protection

Only install an anti-virus program from a known and trusted source. Keep virus definitions, engines and software up to date to ensure your anti-virus program remains effective.

### Back up your data

Back up on a regular basis – if you are a victim of a security incident, the only guaranteed way to repair your computer is to erase and reinstall the system.

### Be careful what you click

Avoid visiting unknown websites or downloading software from unknown or untrusted sources. These sites often host malware that will automatically, and often silently, compromise your computer. If attachments or links in email are unexpected or suspicious for any reason, don't click on them.

### Never leave devices unattended

The physical security of your devices is just as important as their technical security. If you need to leave your laptop, phone or tablet for any length of time – lock it up so no one else can access it. For desktop computers, shut down the system when not in use.

### Protect sensitive data

- Avoid storing sensitive data (e.g., Social Security numbers, credit card information, family records, health information, etc.) on your computer, laptop and mobile devices.
- Securely remove sensitive data files from your system when they are no longer needed.
- Always use encryption when storing or transmitting sensitive data.

### Use mobile devices safely

Considering how much we rely on our mobile devices, and how susceptible they are to attack, you want to make sure you are protected:

- Lock your device with a PIN or password– and never leave it unprotected in public.
- Only install apps from trusted sources.
- Keep your device's operating system updated.
- Don't click on links or attachments from unsolicited emails or texts.
- Avoid transmitting or storing personal information on the device.
- Most handheld devices are capable of employing data encryption – consult your device's documentation for available options.
- Use Apple's Find my iPhone (https://support.apple.com/explore/find-my-iphone-ipad-mac-watch) or the Android Device Manager (https://support.google.com/accounts/answer/6160491?hl=en) tools to help prevent loss or theft.
- Back up your data.

### Additional tips to help keep you safe and secure online:

- Use a firewall – Mac and Windows have basic desktop firewalls as part of their operating system that can help protect your computer from external attacks.
- Use public wireless hotspots wisely.
- Be conscientious of what you plug in to your computer. Flash drives and smart phones can contain malware.
- Be careful of what you share on social networking sites.
- Monitor your accounts for suspicious activity.
- Bank or shop online only on trusted devices and networks. Make sure to log out of these sites when you complete your transactions.

### Sign up for paperless statements

Switching to paperless statements provides multiple benefits and reduces the risk of having statements stolen in the mail. It's easy to do.

Why you should consider switching:

- Paper statements, bills and other documents can be intercepted in the mail by identity thieves.
- Secure paper disposal and shredding isn't necessary.
- You can receive your statement even if you move without worrying about it getting lost or sent to the wrong address.

**Corporate Headquarters**
99 Park Avenue, 4th Floor | New York, NY 10016
212 659-0600 | www.MetropolitanBankNY.com

Member FDIC | EQUAL HOUSING LENDER