# EagleNews

EAGLEBANK


Because cyber crime is such a threat to our personal and business finances and identity today, we are giving it full attention in this newsletter. Understanding cyber crime starts with understanding the steps we need to take for protection, as well as the subtle, yet often bold schemes and tricks criminals use to pull us into their web of thievery. Education is the important first step. All employees in an organization must be on the defensive and know what to look for, what to do, and most importantly, when something is suspicious, to act quickly. Cyber threats and tactics are consistently changing and adapting to circumvent mitigating controls and security measures, so it's important that organizations know how to recognize potential threats and be prepared.

Constant vigilance is essential to security controls, procedures, and training—and critical to safety. Some very basic safeguards, if practiced by everyone in an organization, can make a dramatic difference. Never share passwords. Keep account numbers secure. Never share information when asked via email, phone call, or text message. Sign out or lock your computer whenever you leave it. Always update your system's anti-virus software. Maintain appropriate internal controls. Check monthly statements for any unauthorized activity. Establish account alerts to notify you when certain activities take place; contact your bank immediately if you suspect a problem. Early detection of fraudulent activity on your account is key to preventing potential financial loss.

At EagleBank, besides our own on-staff IT and security specialists, we work with experienced cyber crime and fraud prevention vendors who provide cutting-edge protection systems to keep your information and your money safe. We deploy sophisticated security measures, such as encryption protocols for data and email; user ID's and passwords; system controls; and intrusion detection and prevention technology. Additionally, time-out and lock-out features are in place to prevent unauthorized access, and we continually train our employees on safeguarding our customers' data. We also work closely with regulators, law enforcement, and industry experts to stay ahead of cyber criminals.

We must work as a team to conquer cyber crime. Working together, we can outsmart the criminals and keep our money and private information safe. Some good basic information follows. We hope you will share this newsletter with everyone in your organization.

Thank you for trusting us with your financial needs. Please be assured, we are working diligently to keep you and your money safe at EagleBank.

## TABLE OF CONTENTS



### Real Estate News

**Sign up for EagleBank Presents the Bisnow Morning Brief**
bisnow.com/morning-brief-washington-dc

### Eagle Bancorp, Inc. Stock

Eagle Bancorp stock is available for purchase through NASDAQ.
Symbol: **EGBN**

### EagleBankCorp.com

Visit for more valuable information, to apply for a job, or read press releases.

## CYBER SECURITY "RED FLAGS"

You play an important role in preventing a data breach or attack that could lead to significant financial loss. Be aware of the following Red Flags that may signal that your computer is infected.

### #1 Incorrect File Extensions

All of a sudden your files contain inappropriate extensions. Typically your files should have recognizable extensions like .doc, .xls, .ppt, and .pdf.

### #2 Antivirus Disabled

An antivirus alert pops up or if you receive a notification that it is disabled.

### #3 Social Media

If you see a post on social media that talks about the bank and mentions anything about a breach.

### #4 Popup Ads

You see pop-up ads while you are online.

### #5 Ransomware Requests

You receive a notification telling you that you need to pay to get your files back.

### #6 Denied Access

You receive "Access Denied" alerts that your computer tried to access files/folders that you didn't try to use.

### #7 Uninitiated Contact from IT

You receive calls and/or emails, and/or visits from IT Support or Network Security regarding unusual activity that you didn't initiate.

### #8 Error Messages

Your computer begins to act strange OR won't boot after a re-start.

### #9 Mouse Moves by Itself

Your mouse begins to move by itself (and you know that the Help Desk isn't logged in remotely).

### #10 Suspicious Devices

There is a device plugged into your computer in the USB or network port (ex. Key Logger or Network Sniffer)

## SPOTLIGHT ON CYBER CRIME

Education Is Key! Cyber Crime is on every organization's mind today. It can be devastating when a cyber thief or a computer virus sneaks into your personal or business email or computer system. Below are some basics to help you and your organization learn more about the enemy.


### WHAT OR WHO IS KNOCKING ON YOUR DOORS?

**Adware:** Software that automatically plays, displays, or downloads ads to a computer; some adware is harmless, but others double as spyware.

**Blended Threat:** A threat that combines different components to attack and propagate itself in several ways.

**Botnet:** A group of compromised computers often used to send SPAM, inappropriate material, and to launch Distributed Denial-of-Service attacks against websites.

**Denial-of-Service:** Often launched by networks of zombie computers or botnets, saturating the victims machine, the DoS threat renders a website or service unavailable to legitimate users.

**Keylogging:** A piece of malware installed on a computer that captures and records keystrokes which are then transmitted to a remote computer.

**Malware:** Software that can replicate itself and infect a computer without the knowledge of the user. It spreads when transmitted by the user over a network, internet or through removal media such as CDs or memory sticks.

**Pharming:** An attack by a hacker with the skills to redirect website traffic to a bogus website using host files or exploiting DNS server software. (DNS server computers resolve Internet names into their real IP addresses).

**Phishing:** A well researched email created by cyber criminals in an attempt to trick employees into divulging login credentials or to load malware.

**SPAM:** Electronic junk email sent to email addresses collected from all over the Internet.

**SPIM:** Spam sent via instant messaging systems such as Yahoo, Messenger, MSN Messenger and others.

**SPIT:** Spam over Internet Telephony - unwanted, automatically-dialed, pre-recorded phone calls using Voice Over Internet Protocol (VoIP). They are also referred to as "Robocalls."

**Spoofing:** An attack from a person masquerading as another.

**Trojan Horse:** Software that conceals a payload (often malicious) while appearing to perform a legitimate action; they often install "backdoor programs" which allow hackers a secret way into a computer system.

# BUSINESS EMAIL COMPROMISE

Business Email Compromise (BEC) may be the most common cyber crime today affecting the Financial Sector today. It requires every organization's attention because it is happening more often. BEC involves criminals who hack business email accounts typically through phishing – often those of top level executives. Once compromised, bogus emails can be sent from the CEO or CFO to wire money – often when that person is out of town and verification is more of a challenge. Keeping information out of the hands of cyber criminals once they've hacked into company email is nearly impossible.

Cyber criminals have many tricks and methods to perform their evil. They often use relatively unsophisticated ways. They manipulate email or create commands that automatically send fraudulent emails to a trash folder or to a hidden folder so they are not visible to the true email account user. They send wire transfer instructions when the CEO or CFO is on official travel, making it more likely that email would be related to the official business and harder to recognize as fraudulent; they mark the wire transfer request as urgent or confidential and state that it must not be discussed with others; they set up a new website and email address that appear almost identical to legitimate business addresses, often by changing only one character; they direct payments to vendors/ suppliers to go someplace else – to the cyber criminals' accounts or to overseas banks.

## Reducing BEC Risk

• Look for any small change to any payee's information; verify it by calling them.

• Limit the number of employees who have the ability to authorize a wire transfer.

• Require dual-approval and set restrictions.

• Take full advantage of security features offered by the bank.

• Verify any email requests involving monetary transactions in peron or through a known phone number.

• Instruct staff to delay approvals when the bank has questions or needs additional verification.

## Learn More About BEC

We offer a brochure that provides more detailed information on Business Email Compromise. Please visit our website at EagleBankCorp.com/security to download this brochure.


# CYBER SECURITY "MORE SUBTLE SIGNS"

**Attachments Not Working**

You've clicked on a link in an email (maybe two orthree times) and nothing happened, or something unusual happened.

**Changes to your Browser or Home Page**

All of a sudden your browser has a new homepage or browser toolbar add-ons.

**Computer Programs Not Working**

Programs that worked yesterday aren't workingtoday.

**Emails You Haven't Sent**

Friends or colleagues say that they have received emails that you haven't sent.

**Excessively Slow or Non-Responsive Internet**

Your Internet browser becomes slow or nonresponsive AFTER visiting a site.

**Excessively Busy Network**

You notice very high network usage (the light onthe Network card blinks almost constantly).

**Excessively Busy Computer Hard Drive**

Your computer hard drive is excessively busy (churning and chattering for minutes at a time).

**Folders You Didn't Create**

You notice folders on your "U:/" that containsfiles that you haven't created or don't use

**Redirected When Searching the Internet**

When you try to visit a website and you notice thatyou're being redirected to another site.

**CAUTION:**

*Never leave your computer unlocked while you're away from your desk.*

# EDUCATION

## Build Your Army Of Cyber Soldiers – Recruit All Employees

Employee Education is the first step in protecting your business, computers, money, and identity from cyber crime. Every employee must be aware, alert, and suspicious of any email that lands in their inbox. All employees, especially those who handle money, need to know:

• No attachment should be opened unless the sender and his/her address looks legitimate and authentic. Hard to tell sometimes...be alert and suspicious! Otherwise the attachment could carry all sorts of nasty baggage. (See list on page 2.)

• Verify ANY email that is asking you to send a wire, send money, or change any vendor address or payment instructions. Call the sender using a number on file or publically available and make sure he/she truly sent the email. Better yet, visit their office ask, (for example) "I'm checking to see if this email to send $90,000 to XYZ is truly from you?" That small effort may save the organization $90,000.

• Examine emails and email addresses for any slight change. Is the grammar, punctuation, and spelling incorrect? Is a sense of urgency implied? Does the conversational tone of the message sound different than the sender's?

• Is the sender out of town or out of the office? If so, be especially suspicious and find a way to contact or verify.

• Verify telephone calls and questions asked by strangers, often misrepresenting themselves as someone or some company you are familiar with. Reveal nothing and act upon nothing until you know and verify who the caller truly is. You can always call them back on a verified number you look up or know to be theirs.

***Quick Tip: Verification is the best way to foil the fraudsters is to say: "Give me your phone number and I'll get back to you with an answer once I share and verify this." This gives you time to research and verify.***

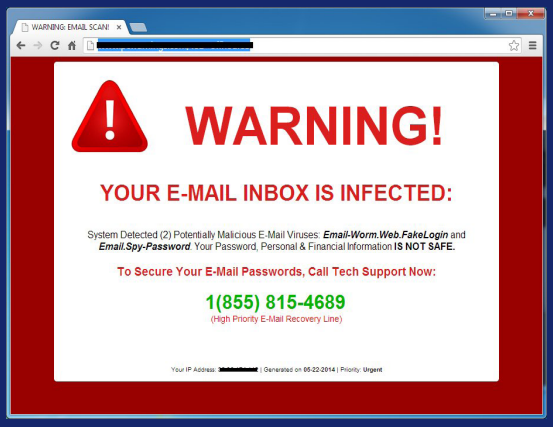
• When in doubt, Hover! By "hovering" over a link in an email, you can see the actual site you will be connecting to.

• Act Quickly! It's not always too late. So, a wire request went to the bank seconds ago. You realize suddenly that the company name was not Happy Times, but Happy Ties! Call the bank immediately! Sometimes the bank can halt the transaction or pull in help to stop the action or apprehend the offender. Time is of the essence.

We're all in this together to detect and minimize the impact of cyber crime. It takes everyone's alert and suspicious behavior and their quick action to fight identity theft or stop a thief, and protect our information and property.

# POP-UPS

**They are tricky little teasers with a message. A message they hope will pull you in and entice you to click and open. Pop-ups appear out of nowhere and usually contain little programs that hop onto your computer when you download something else. They are often hidden in a licensing agreement of other software or sites you download or click into. They are used by advertisers to track your Internet searches and shopping, but some more dangerous ones can bring with them a Trojan horse that unloads other malicious applications or a key-stoke-logger bug with the ability to access confidential data and passwords. Best defense is to invest in quality internet protection software. Always avoid pop-ups and suspicious attachments to emails. Be alert and suspicious of anything that asks you to open, download, or send something. Look for address errors, language irregularities and a sense of urgency to act now. They are often hard to detect, especially the newer pop-ups, so a quality software package is your best option to avoid them.**




# SPYWARE

**Spyware is a program that attaches to your computer and oversees and tracks what you do and where you go in cyber space. It then relays this information to a separate third party. Spyware is illegal without your consent, but you often inadvertently agree to installing it in return for "free" software from the internet. Your consent to install the spyware is "hidden" deep down in the fine print of the End User License Agreement. The most common types of spyware send your online user habits to media companies. In some cases, it can record what you type, including passwords and credit card number. It can also affect the computer's performance or damage a computer's operating system. Most good, trusted anti-virus software applications focus on spyware as well as the other menaces attacking your computer.**

# MORE CAUTIOUS – MORE PROACTIVE

The aftermath of the massive Equifax computer hack, is providing us with more cautions and security steps to implement: (1) Not planning any major purchases? Place a credit freeze on your credit cards by notifying the three credit bureaus (Experian, Equifax and TransUnion). (2) Set up fraud alerts with each of the credit bureaus that will tell you if anyone is trying to apply for credit under your name. (3) Sign up for credit monitoring; many private companies offer this service today. (4) Keep an eye on your taxes; file early; and convey your concerns to the IRS that you want to be sure no one else is filing under your name and social security number. (5) Be suspicious of schemers claiming to "help" or "offer assistance" where a potential hack or security breach is involved. Question everything and trust no one that you don't contact or verify on your own, outside the email or the offer to help.

Below are some precautions for you to consider:

## BE EXTRA CAREFUL ABOUT EMAILS AND LINKS

Avoid clicking on links or downloading attachments from suspicious emails that claim to be updates from Equifax or connected to the breach. Equifax will send paper mail to consumers whose credit card numbers or dispute documents with personally identifying information were impacted.a

Hackers often use news of big breaches to conduct "phishing" campaigns, sending official-looking emails that make it seem as if the affected company or other legitimate services are asking them to supply information or click through to a link to repair any damage.

When in doubt, call or email the company that appears to be sending the message separately, don't go through the email you've been sent.

## PLACE A FRAUD ALERT ON YOUR ACCOUNT

Place a "fraud alert" on your credit reports and review the reports carefully. A fraud alert is a signal placed on your credit report to warn potential creditors that they must use "reasonable policies and procedures" to verify your identity before they issue credit in your name.

## CHANGE PASSWORDS

Especially consider this if you typically use similar passwords and security questions on multiple accounts. Once hackers have access to ID and password information for one system, they routinely try the same combination against multiple other platforms to see which ones work, an easily automated process. It is important to use different passwords for all of the online site you visit.

## ENABLE TWO-FACTOR AUTHENTICATION WHEN ACCESSING ONLINE ACCOUNTS

Cyber criminals often use this information gathered to answer your "security questions" and reset your password.

Two-factor authentication keeps them from doing that by sending a text message or call to the user's phone with a code as a second verification step. The code must then be typed in before the account page can be opened.

Also consider enabling additional security features such as alerts, limits, etc.

## CHECK YOUR CREDIT CARD AND OTHER ACCOUNTS

Review your online and paper statements for suspicious activity. That includes banks, credit card companies and hotel and airline loyalty programs.


At EagleBank, we take cyber security very seriously and hope this additional information is helpful to you. EagleBank systems were not affected by this Equifax breach, but we share these pointers as part of our Relationship F-I-R-S-T approach. You can find more information about fraud and cyber security at www.eaglebankcorp.com/security.

If you have any questions or concerns, please do not hesitate to contact EagleBank Customer Care at 301-628-4708.

## FOCUSED ON SECURITY

# RANSOMWARE

This is a malicious software (malware) that encrypts files with a key known only to the cyber criminal. The victim is then extorted to pay a sum of money (usually in Bit Coin) to the criminal in return for the decryption key. As often as not though, the cyber criminal never gives the victim the decryption key. It can corrupt personal and business files, leading to stolen data, system outages and large financial losses. Here's how to avoid it and protect you and your organization.

- Always back up your files and save them offline or in the cloud.
- Always use antivirus software and a firewall that are both set to update automatically.
- Enable Pop-up blockers. Pop-ups are a true disease transmitter.
- Think before you click. Be cautious when opening emails or attachments you don't recognize, even if the message appears to come from a company or a person you know. Impersonation is an easy trick for criminals. Look for the site address on banner ads. Visit through your browser rather than clicking on it from the ad.
- Only download software from sites you know and trust; you can always do a search and go directly to the software site and download from there on your own.
- Alert your local law enforcement agency as soon as you encounter a potential attack or cyber crime website.

# ADDITIONAL RESOURCES

Online Safety:
www.usa.gov/online-safety

FBI Internet Crime Complaint Center:
www.ic3.gov/default.aspx

Identity Theft:
www.fbi.gov/investigate/white-collar-crime/identity-theft

Safe Internet Banking/FDIC:
www.fdic.gov/bank/individual/online/safe.html

## DIRECTORY

**Ron Paul**
Chairman & CEO
301.986.1800

**Susan Riel**
Sr. EVP & Chief Operating Officer
240.497.1667

**Tony Marquez**
EVP, Chief Real Estate Lending Officer
240.497.1799

**Lindsey Rheaume**
EVP, Chief C&I Lending Officer
240.497.2951

**Alexis Santin**
SVP, Treasury Management
202.292.1610

**Maria Acosta**
SVP, Commercial Deposit Services Manager
202.292.1633

**Mark Deitz**
SVP, Residential Lending Area Sales Manager
240.406.1152

**Chaz Sowers**
SVP, Director of Information Security
301.375.4507

**Jane Cornett**
VP, Corporate Secretary
240.497.2041

## BRANCHES

**Virginia**

Alexandria, 277 S. Washington St. | 703.956.5075

Ballston, 4420 N. Fairfax Dr. | 571.319.4800

Chantilly, 13986 Metrotech Dr. | 703.378.0010

Dulles, 45745 Nokes Blvd. | 703.230.1515

Fairfax, 11166 Fairfax Blvd. | 703.359.4100

Merrifield, 2905 District Ave. | 571.319.4900

Reston, 12011 Sunset Hills Rd. | 571.319.4848

Rosslyn, 1919 N. Lynn St. | 571.319.4855

Tysons Corner, 8245 Boone Blvd. | 703.752.9360

**Maryland**

Bethesda, 7815 Woodmont Ave. | 240.497.2044

Chevy Chase, 5480 Wisconsin Ave. | 301.280.6800

Park Potomac, 12505 Park Potomac Ave. | 301.444.4520

Rockville, 110 N. Washington St. | 301.738.9600

Rollins Ave./Rockville, 130 Rollins Ave. | 301 .287.8500

Shady Grove/Rockville,9600 Blackwell Rd. | 301.762.3076

Silver Spring, 8665-B Georgia Ave. | 301.588.6700

**DC**

Dupont Circle, 1228 Connecticut Ave., NW | 202.466.3161

Gallery Place, 700 7th St., NW | 202.628.7300

Georgetown, 3143 N St., NW | 202.481.7025

K Street, 2001 K St., NW | 202.296.6886

McPherson Square, 1425 K St., NW | 202.408.8411

---

Corporate Headquarters
7830 Old Georgetown Road, 3rd Floor
Bethesda, MD 20814

---

Eagle Commercial Ventures
Tony Marquez | 240.497.1799

Eagle Insurance Services
Ken Van Valkenburgh | 240.497.2061

Investment Advisory Services
Larry Bensignor | 240.497.1788

MD Lending Team | 240.497.2049
DC Lending Team | 202.292.1624
VA Lending Team | 703.277.2200

Operations Center, Tech Rd., Silver Spring | 301.986.1800

Residential Mortgage Lending | 301.738.7200

---

**Main Number**
301.986.1800

**Electronic Banking Service**
301.628.4708