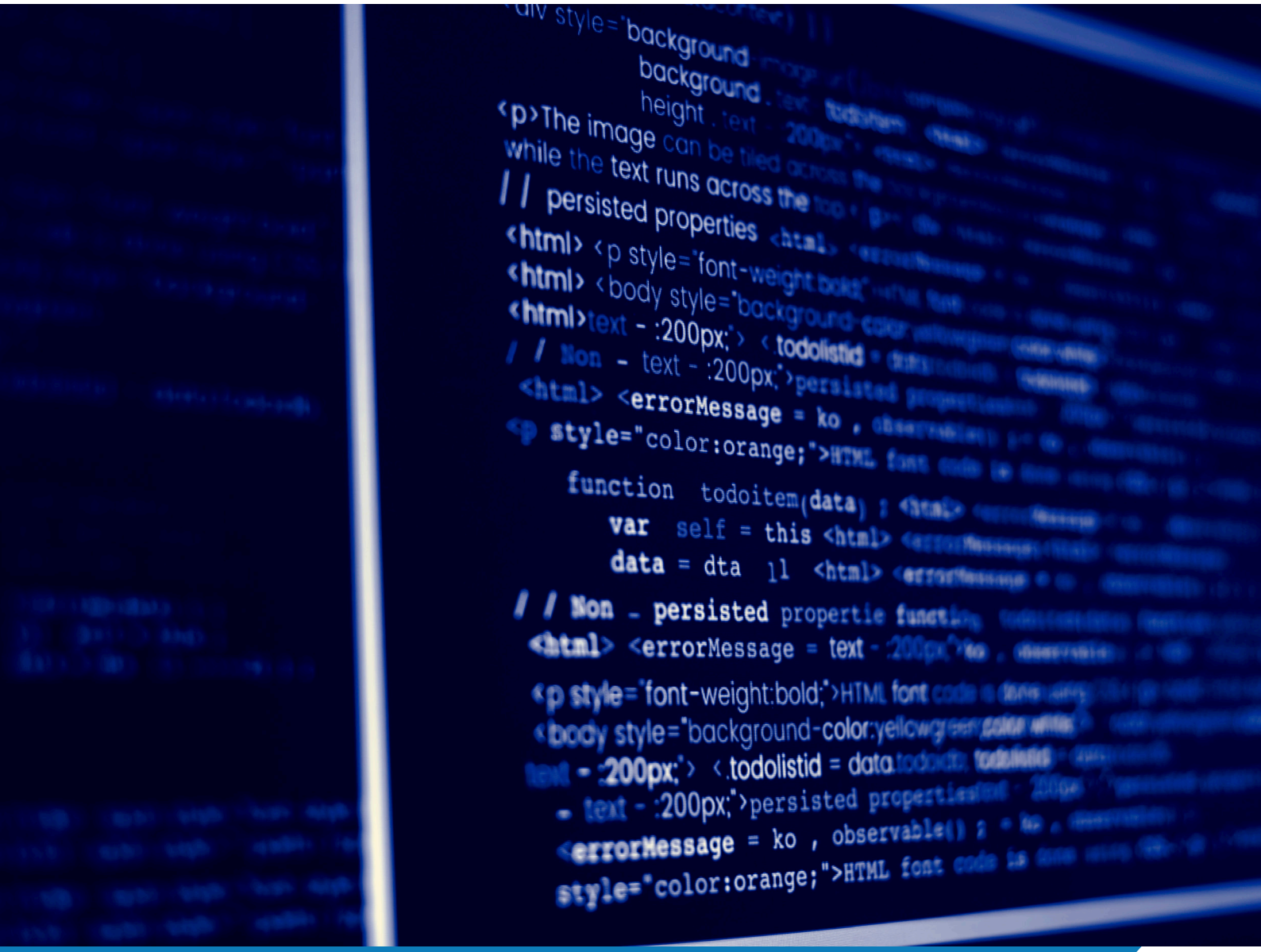
PBMares
Your Future. Our Focus.



# Cybersecurity with a Remote Workforce

The COVID-19 pandemic has caused more and more people to work from home. The increased use of collaboration and cloud technologies have enabled employees to stay productive, but have increased the risk of phishing attacks, online fraud and cyber attacks. In this document, we'll cover the most popular cybersecurity threats and provide tips on mitigating them.

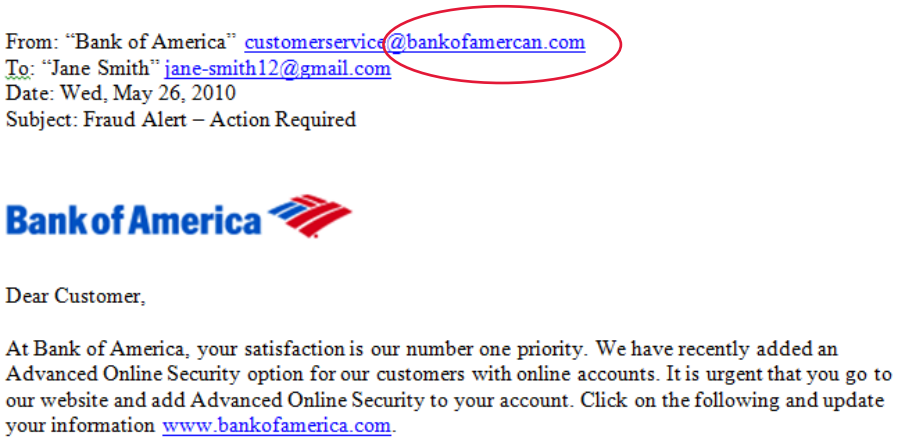
# Phishing Attacks

Phishing attacks have increased in recent months because there are simply more opportunities for criminals to impersonate legitimate organizations. The coronavirus pandemic has caused most companies to increase correspondence with prospects and customers. With so many emails, an unsuspecting recipient may unknowingly click on what seems to be a legitimate email. A link click or attachment download from a phishing email may lead to revealing your username and password or installing malware that steals company secrets.

So let's talk about how to identify a phishing email.

Let's say you receive an email that on the surface seems legitimate. It will probably be branded to an organization that you recognize in order to gain your trust.

Look at the sender's email address. If the email is from Bank of America, then the domain of the sender's email address should be bankofamerica.com. If it isn't, that's a red flag.



From: "Bank of America" customerservice@bankofamercan.com
To: "Jane Smith" jane-smith12@gmail.com
Date: Wed, May 26, 2010
Subject: Fraud Alert – Action Required

Bank of America

Dear Customer,

At Bank of America, your satisfaction is our number one priority. We have recently added an Advanced Online Security option for our customers with online accounts. It is urgent that you go to our website and add Advanced Online Security to your account. Click on the following and update your information www.bankofamerica.com.

Some scammers try to fool you by making the email domain look legitimate. If there are multiple periods in the domain of the email, make sure you correctly identify which part is the actual domain. For example, the email address john@bankofamerica.eprs.com is not from bank of america. It's from eprs.com.

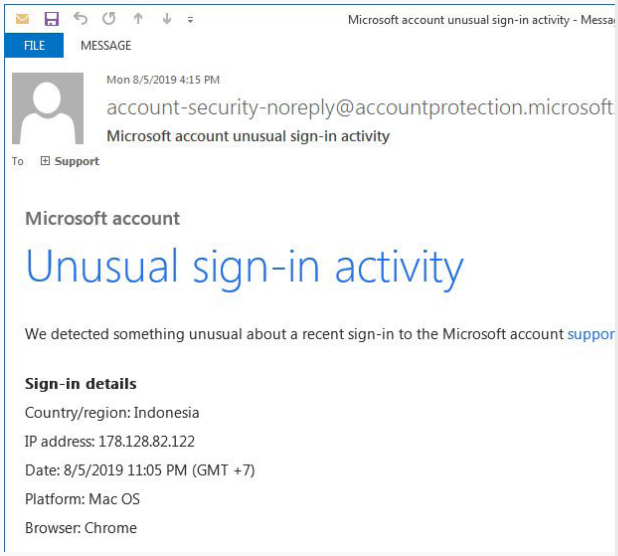
Let's say you accidentally click on a suspect email link. It may take you to a webpage that looks legit but really isn't. Be sure to look at the URL in your browser before providing any login credentials or doing anything further. Make sure the domain is legitimate, just like you did with the sender email address. If the domain is legitimate, make sure you have a secure connection to the site, which will be displayed in the browser.

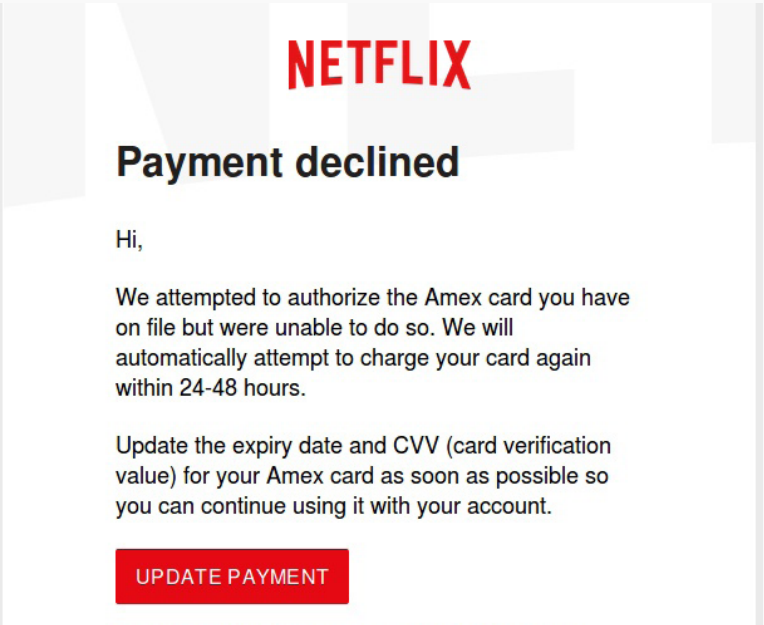
Phishing emails often try to elicit fear or urgency. Cybercriminals will tell a story to trick you into clicking a link or opening an attachment. They prey on urgency or an individual's fear. Examples include:

- Notifying you of a recent purchase that you did not make.
- Alerting you to suspicious activity on your account.
- Indicating a problem with your account or payment information.
- Sharing critical information about cures for the COVID-19 virus, or urgent information from government entities.

Phishing emails often contain a generic greeting such as "To our valued customer" or "Dear Sir". A company that you're working with will know your name, so this is a red flag. Phishing emails also frequently have misspellings or language within the email that doesn't seem quite right.
Here are a few simple guidelines to protect yourself from phishing emails:

- Don't click on links within emails or open attachments from people you don't know.
- Don't respond to an unsolicited request from companies you work with; if there is a concern, contact the company directly using information on their website.
- Be especially cautious when making online financial transactions. Make sure the website is legitimate and the site is secure.
- Don't provide personal or company information when contacted via email or telephone. Instead, use a verified email address or phone number to contact the person directly and confirm the legitimacy of the request.
- Finally, trust your instincts. If an email does not seem quite right, delete it and contact the sender directly to verify the email.



# Voice Phishing

With voice phishing, a criminal may call into customer service or another department and impersonate an actual customer. In these situations, the criminal may have some basic information about the person they are impersonating in order to gain trust. They may ask for help in resetting an account or password. Having solid policies and procedures on authenticating a caller are really important for this type of situation. Also, it's important to have guidelines on sharing information even after authenticating the caller. For example, if you are resetting a password or account, then send a reset link to the email address you have on file for the individual instead of providing their new password over the phone.

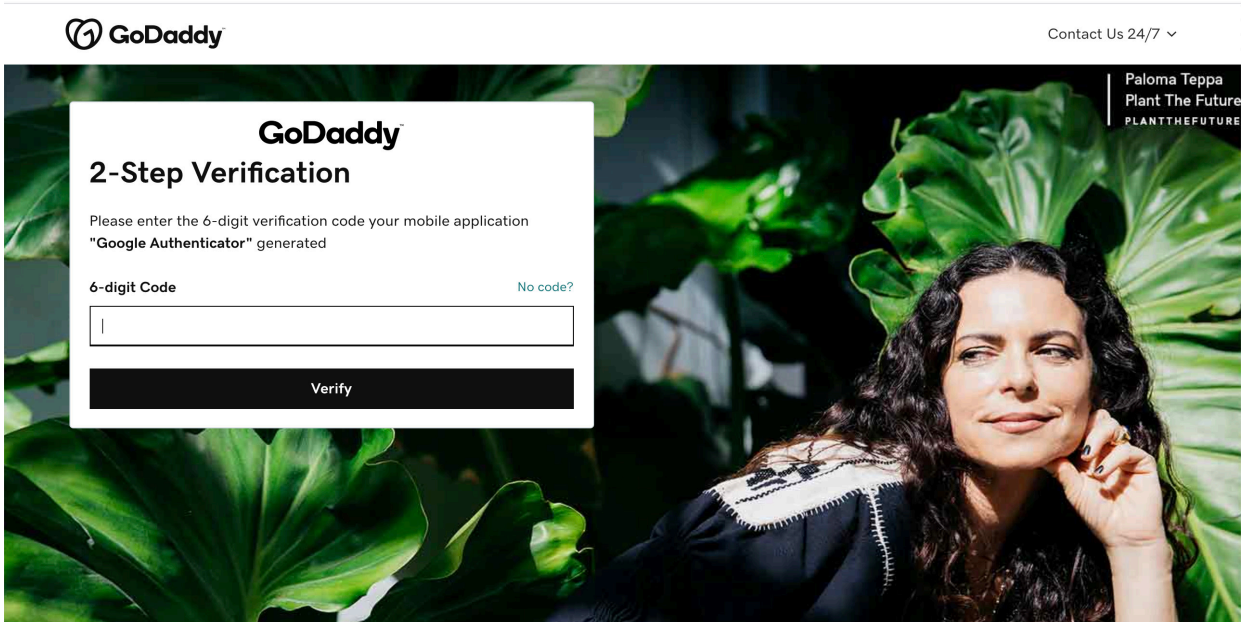
# Saas Active User Management

In addition to threats from unknown cybercriminals, you also face threats from people you know. It's important to review all of your software applications and the active users accounts. More often than not, companies forget to remove security access for former employees and contractors, which can create a big hole in your security. Plus, if they are still an active user on a saas application, that user account is probably costing you money. So review all accounts, disable former employees and review the security settings for those who do still have access.

# Poor Password Management

Too many people not only use weak passwords, but use the same password across multiple accounts. Every employee should have a password manager and you should consider deploying an enterprise level password management system such as Lastpass for business or Dashlane for business. These systems enforce the creation of strong passwords and enable a business to securely manage passwords across all departments and employees.


# Two Factor Authentication




Most sites with sensitive data offer two factor authentication, which we highly recommend. Basically, this adds a second layer of protection over and above your username and password for any given site or software. Two factor authentication creates a two-step process to logging into a site. First, you login as usual with your username or password. Then, the site requires you to authenticate in a second manner.

The site may send a text message to your phone with a code that you enter into the site. Some sites work with a mobile authentication app such as Google Authenticator that provides a code through the app instead of having a code sent via text.

By requiring a second form of authentication, you are able to further secure access to your sensitive accounts and information

# Home Wifi Protection

Since so many employees are working from home, let's discuss home wifi and security. Your home wifi is served up by a wifi router and that router holds the name of your wifi network, also known as the SSID. We suggest changing the default name of your Wi-Fi network because an attacker may be able to tell what type of hardware you have, and its vulnerabilities, based on the pattern of the default name. When changing the network name, use a name that is not personally identifiable. Don't name your network Smith Family Wifi or 4350 Main Street.

And if you're changing the network name, be sure you have a strong and unique password for your wifi.

In order to change the name and password for your wifi network, you'll have to login to the administrative control panel of your router. We suggest making sure that the password to access the router's control panel is also strong and unique.

Wireless networks come with multiple types of encryption standards, such as WEP, WPA or WPA2. We highly suggest choosing WPA2 because it is the most secure of the three. If your router only has WEP or WPA, then it's probably old and should be replaced. If your router has WPA3, which is the latest security standard, you can use it as long as all of your connected devices support the same standard.

There are certainly other steps you can take to further secure your home, but those few steps will go a long way.

## Software Updates and Anti-Virus Software

Be sure to update your software not only on your computer, but also on connected devices such as phones as soon as updates are available. Quite often software updates contain important security patches to recently discovered vulnerabilities.

And for one final tip, make sure you are using anti-virus and malware scanning software on all computers. This software can help defend against threats such as viruses and ransomware. You might consider looking into software such as business editions of Norton Security and Malwarebytes to help in this area.


# Final Thoughts

By following these tips and guidelines, you'll help protect yourself and your company from costly cyber attacks. Remember, most employees aren't purposely negligent when it comes to security; they just need a reminder about the best practices to follow during this stressful time. If you have any questions or need assistance with your specific situation, please contact our office. Our experts are always here to help.

# About PBMares, LLP

PBMares, LLP is an accounting and business consulting firm serving U.S. and international clients, with offices in the Mid-Atlantic. The firm unlocks opportunity for clients using the right balance of industry, specialty and general business services in the areas of audit and accounting, tax planning and preparation, pension plan design/ administration, and owner-managed/corporate financial consulting. In addition, the firm provides additional services through its affiliates: Artifice Forensic Financial Services, LLC, a financial consulting division specializing in fraud investigations and forensic accounting; PBMares Wealth Management, LLC, a registered investment advisor; and TMDG, LLC, a national healthcare consulting firm specializing in medical claims audits. More information is available online at www. pbmares.com.community-based initiatives.


PBMares, Headquarters
701 Town Center Dr.
Suite 900
Newport News, VA 23606

(757) 873-1587

pbmares@pbmares.com

www.pbmares.com/locations

**Fairfax (Metro DC)** (703) 385-8577
**Fredericksburg** (540) 371-3566
**Harrisonburg** (540) 434-5975
**Morehead City** (252) 726-0551
**New Bern** (252) 637-5154
**Newport** (757) 873-1587
**Norfolk** (757) 627-4644
**Richmond** (804) 323-0022
**Rockville** (240) 499-2040
**Warrenton** (540) 347-4970
**Williamsburg** (757) 229-7180
**Wilmington** (910) 762-9671