Mobile Banking App is HERE!

UNION BANK

September 2017

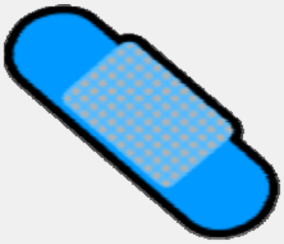
Volume 3 Issue 9

You Are Going to Need to Patch That Up!

You've most likely heard the word "patches" several times when discussing IT, and with good reason. Patches are one of the most important cybersecurity tools to help protect against malware and viruses, and as such, is definitely worth revisiting.

The History

In the past, software suppliers sent patches on paper tape or on punched cards to be cut out and "patched" into the original media. We have since come a long way. Today, patches are a piece of software designed to fix and/or update existing software. Patches include fixing vulnerabilities and bugs and improving design, performance and userability. Deploying patches has also become easier and more efficient since the paper tape and punch card days. Now with the Internet, you can download patches from the developer's website or through automated software updates.



Security Patches

There are several types of patches, however security patches are one of the most important. The security patch is usually dispatched to fix specific problems related to the product installed on devices, such as computers, smartphones, or tablets. Depending on the severity, the program developer may label these patches as "critical," "important," "moderate," or "low." These patches eventually lead to better performance of that application, and of course, more security. Sometimes, patches are available through your antivirus or antispyware application which is why it is so important to make sure those applications are always kept up-to-date. This is not only important for your PC or laptop, but also for your smartphones and tablets. The notifications that you receive on your device for app updates are crucial to maintaining your security. Some app updates are automatic and some may require you to manually update them. Regardless of the method, these updates are recommended to make sure any recently discovered bugs are taken care of.

Preventative Measures

Patches provide preventative maintenance. Just like you change the oil in your car every three to six months to make sure the engine is running at optimal condition, the same concept applies to your computers and other electronic devices. Software developers are constantly researching and trying to be one step ahead of hackers. If they see a possible security gap, they fix it before a threat even presents itself.

Updates

Another type of patch is one that provides updates to the graphics, layouts, text and other features, in the end, enhancing your user experience. With these patches, you can enjoy the newest versions of the software.

Although receiving these update notifications may be a nuisance, keep in mind that, in the end, these are designed to protect you and your information. These patches help fix potential problems, provide security and enhance usage. So be sure to stay up-to-date with your patches and your updates and help protect your data.

Sources:
http://www.idtheftcenter.org/Cybersecurity/what-are-security-patches-and-why-are-they-important.html
http://www.toptenreviews.com/software/articles/pc-security-and-the-importance-of-patch-updates/
https://community.norton.com/en/blogs/norton-protection-blog/importance-general-software-updates-and-patches

Middlebourne Office
103 Dodd Street Middlebourne, WV 26149
304-758-2191

Sistersville Office
700 Wells Street Sistersville, WV 26175
304-652-3511

St. Marys Office
401 Second Street St. Marys, WV 26170
304-684-2427

Hundred Office
3924 Hornet Hwy, Hundred WV 26575
304-775-2265

Ellenboro Office
90 Main Street Ellenboro, WV 26346
304-869-3232

Harrisville Office
1500 E. Main Street Harrisville, WV 26362
304-643-2974

Pennsboro Office
214 Masonic Ave. Pennsboro, WV 26415
304-659-2964

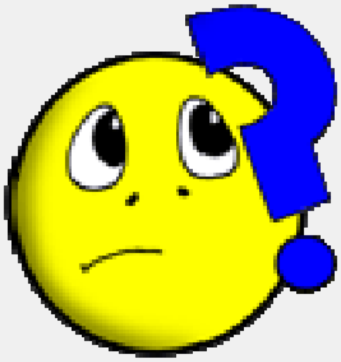
Marietta-Loan Production
Kroger Plaza 19 Acme Street Marietta, OH 45750 740-374-0010
This is not a full service location. Deposits/withdrawals cannot be processed at this location.

New Martinsville Office
638 N SR 2 New Martinsville, WV 26155
304-455-2967

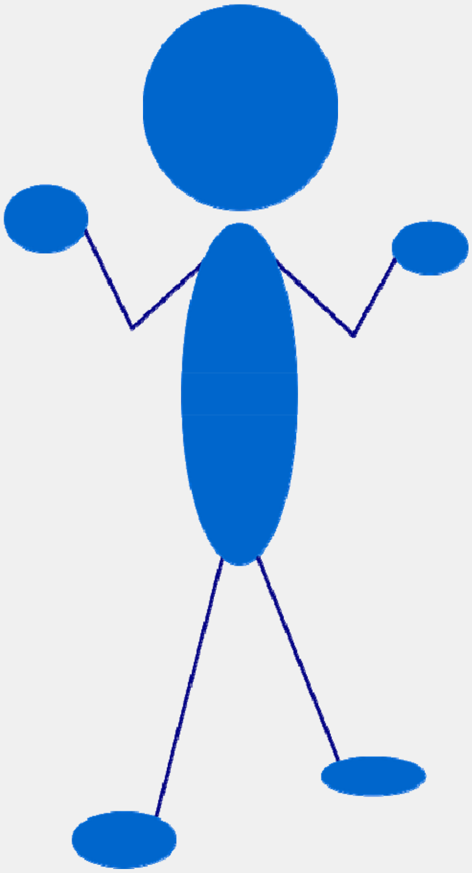
In this issue:

You’ve Been Hacked; Now What?

If your computer has ever been hacked, take comfort in knowing that you are definitely not alone. Forty-seven percent of Americans have had their personal information compromised in one way or another in the past twelve months. The belief that being hacked only happens to big corporations like Target, Sony or eBay, is far from the truth. Many everyday citizens, unfortunately, have their personal computers compromised; and a lot of times, it’s through the hacking method of choice: phishing emails.



Phishing emails are fraudulent emails sent to recipients that contain links to dangerous malware or viruses, all with the goal of stealing personal and confidential information. Hackers have honed their skills to make scam emails look absolutely legitimate. Many times the emails appear to come from a well-known source such as your bank, utility company or other trusted company. Moreover, you may not even be aware that you have been hacked, because sometimes a virus can run in the background of your PC without raising any major red flags. The loss of your personal information is extremely serious and can cause a ripple effect of other problems. So how do you know if you have been hacked? And what do you do about it? Here is a list of telltale signs and steps you can take to limit the damage.



1. First things first, if you feel that something is amiss, you are probably right. Change your passwords immediately. This means email passwords, banking accounts and everything else. Make sure your passwords are strong and include different special characters, numbers, etc. Be sure to monitor all your accounts on a regular basis, going forward, and look for any strange activity. Immediately report anything that was not authorized.
2. You get a fake antivirus message via email requesting you to take some unusual steps to alleviate the possible “threat.” These kinds of messages are classic signs you have been hacked. Unfortunately, by the time you get this kind of message, the damage has already been done. What to do? As soon as you see the fake antivirus message, shut down your computer and reboot in safe mode. Try to uninstall the unwanted software and follow up by running a complete antivirus scan.
3. You start getting frequent and random pop ups. This might be one of the most annoying signs that your PC has been compromised. What to do? Most of the time the pop ups stem from bogus tool bars. Try removing all unwanted tool bars and resetting it back to the default and update software with the newest version.
4. Your friends and family received strange emails from your account. If only a few people from your email list got the emails, then most likely your computer has not been infiltrated with an email malware. But if everyone in your list got the emails, there is a problem. What to do? Check your computer for any unwanted installed programs and uninstall them. Then run a complete antivirus scan on your computer.
5. You notice odd icons on your desktop. Desktops are prime real estate for cyber criminals. But whether you keep your desktop clean or have it cluttered, always pay attention to strange icons or programs that you don’t remember installing. What to do? Uninstall any unwanted icon and programs. Then run a full antivirus scan.

Remember, technology is changing every day and cyber criminals are becoming bolder with their tactics. If something looks odd, chances are there’s more behind it. Always be alert and think before you click!

Sources:
http://www.phishing.org/10-ways-to-avoid-phishing-scams
https://www.usatoday.com/story/tech/2016/12/15/how-prevent-phishing-scams/95446030/
https://us.norton.com/internetsecurity-online-scams-what-to-do-when-you-fall-for-an-email-scam.html?