Bits of Bytes

Newsletter of the Pikes Peak Computer Application Society, Colorado Springs, CO

Volume XLI | October 2021 | Issue 10

Next P*PCompAS meeting: Saturday, 2 October 2021
We will either have an APCUG presentation about genealogy or highlights from the APCUG roundtable on in-person, hybrid, or online meetings.

The Prez Sez

by John Pearce, President, P*PCompAS

Back in February and March of this year, time seemed to just stand still. Now, time seems to be moving too quickly. I have two PrezSez columns remaining before my term ends, Microsoft Windows 11 is set to be released on October 5th, and a new perpetual license version of Microsoft Office is also set for release on the same date. The Nominating Committee will formally announce the slate of candidates for 2022 at the November meeting with the election held at the December meeting.

VP Cary Quinn is planning another presentation from APCUG. The first choice is a presentation by Sue Mueller on The Frugal Genealogist. The alternative is highlights from the APCUG roundtable on In-person, Hybrid or Online meetings. The next membership meeting is at 9 AM MT, October 2nd, at Springs Community Church. The meeting will also be available via Zoom. Current plans are to collect dues for 2022 starting at the December meeting. Dues remain $1 per year.

There were fourteen people at the last Digerati breakfast. We had another wonderful server and the tables in the meeting room were ready for us. The next Digerati breakfast gathering will be October 16th. It would be great to continue having fourteen or more people for the breakfast each month. Many thanks to Joe Nuvolini for making the arrangements. ☺

Meeting Minutes

by Greg Lenihan, P*PCompAS Secretary

President John Pearce began the 7 August 2021 hybrid membership meeting at 9:00 am. David George provided coffee and John Pearce brought doughnuts. A $1 contribution is requested for coffee from members. A motion was made to approve the minutes from August and they were unanimously approved.

OFFICER REPORTS

Vice-President Cary Quinn said we have a presentation today. Cary was questioned about the best way to reach him and he said text or phone. He only checks e-mail occasionally.

Secretary/Newsletter Editor Greg Lenihan announced the next newsletter deadline as 18 September. The newsletter went out this month without any delivery problems.

Treasurer Toni Logan said the club paid Ann Titus $24 for badge expenses. We have $2931.45 in savings and $161.29 in checking for a total of $3068.74.

Membership Chair Ann Titus had nothing to report.

BOD Chair/Nominating Chair/ Librarian Paul Godfrey had nothing to report for the library. Paul reported the BOD met two months ago. He has been soliciting nominations for officers.

APCUG Rep Joe Nuvolini said we would be pulling the audio from our meetings from the website because they are published in the newsletter.

OLD BUSINESS: None

NEW BUSINESS: None

ANNOUNCEMENTS

The next social breakfast meeting will be Saturday, 18 September.

Our next membership meeting is on 2 October.

AROUND THE ROOM

Paul Godfrey said the fan in his desktop power supply stopped working. He was told they can be replaced but it is a lot easier to buy a new power supply. Paul wondered if the chip shortage affected computer memory, and it was suggested he check crucial.com.

Toni Logan bought an On the Go (OTG) connector for her iPad. Now she can connect a flash drive to the iPad after loading a files

Continued on page 3

In This Issue

Articles

P*PCompAS

Officers

President: John Pearce
jlpnet@comcast.net

Vice President: Cary Quinn
cary.quinn@gmail.com

Secretary: Greg Lenihan
glenihan@comcast.net

Treasurer: Antoinette Logan
antoinettelogan@gmail.com

Staff

APCUG Rep/Webmaster: Joe Nuvolini
Barista: David George
Drawings: Cary Quinn
Editor: Greg Lenihan
Librarian: Paul Godfrey
Membership: Ann Titus

Committees

Audio: A.J. Whelen
Hospitality: Vacant
Programs: Cary Quinn
Publicity: Cary Quinn
Nominating: Paul Godfrey, Ann Titus, & Harvey McMinn

Board of Directors

Paul Godfrey
Ann Titus
Harvey McMinn
Jeff Towne
A.J. Whelan

John Pearce leading the 4 September membership meeting with Zoom attendees in the background.

Those physically present at the 4 September "hybrid" membership meeting

Digerati attending the breakfast at Perkins on 18 Sept. Thanks to Cary for taking the picture.

What is Cryptocurrency?

by Fergus O'Sullivan, reprinted with permission from HowToGeek.com
Original article at: https://www.howtogeek.com/748405/what-is-cryptocurrency/

Chances are you've heard of cryptocurrency: Bitcoin, Ethereum and Dogecoin have all become words we hear on the news or read online. But what is cryptocurrency exactly, and how does it work?

Cryptocurrency vs. Regular Currency

Right now, you hopefully have some money in your pocket in the form of dollars, euros, or rupees, depending on what your country gives out as currency. This money is given value by a delicate system operated in part by governments, as well as certain market mechanisms that are too involved to get into here. This article from *The Balance* serves as a solid primer, though.

Cryptocurrency is different from this, and radically. Instead of having a physical presence—the notes and coins in your pocket—it exists entirely digitally, without the power of a government to back it. Rather, it relies on free-market mechanisms to determine its value: what people are willing to pay for it determines what it's worth.

Of course, without a central issuing authority inflation could become a real issue: anybody could just claim at any time that they have a thousand or a million cryptobucks, and there's nothing anybody could do to stop them. If you create your own U.S. dollars, you'll get arrested for counterfeiting. If you create cryptocurrency out of thin air, nothing will happen.

The Cryptocurrency Blockchain

This problem was one of the biggest issues surrounding cryptocurrencies until Satoshi Nakamoto—likely a pseudonym for a person or group, nobody knows for sure except Satoshi—came up with the blockchain. It's a pretty

Continued on page 4

Meeting Minutes (Cont. from page 1)

app to the iPad. She was only semi-successful in loading some pictures. These were JPG, but they may have JPEG in the name, which may be the problem. Cary had trouble with an OTG cable and had to reformat some flash drives. Last month, Toni reported problems accessing the Gazette on her iMac with Safari. She updated the Mac operating system and now can open the Gazette with the Edge browser (Mac version).

Harvey McMinn said he never had a power supply burn out but they have stopped spinning. If they have bearings, you can pull off a rubber plug and oil them. He sometimes has success blowing them with canned air to get the fan spinning.

John Pearce told us October 5th would be the Windows 11 release date, and if you remember Windows 10, it may take a while to get to you. You can get it as a member of the Windows Insider program, but you need the proper hardware configuration. HP and Dell are offering PCs for pre-order with Windows 11 installed.

Joe Nuvolini used TeamViewer in Italy, and twice in the past week he walked over to his computer and found the TeamViewer screen displayed. He decided to uninstall it.

Jim Miller deleted a file with a TIB extension (Acronis True Image) and tried to recover a backup. He ended up using an older version on another drive to reinstall it. Cary thought maybe he deleted a differential or incremental file, which would not allow it to restore. Joe told a story where he had a problem with Acronis, and went on their website, and downloaded the final version, which fixed his problem.

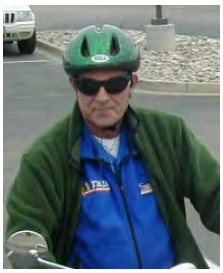
Jeff Towne told a Covid story. He and his wife went to Estes Park for the weekend with a camping group, and both felt bad afterwards. Both had been vaccinated (about eight months ago), but both tested positive for Covid. His wife is still in the hospital with lung issues. This kicked off a long discussion on Covid.

PRESENTATION

Cary Quinn showed several videos from APCUG members. The first was Ron Brown's (Tech for Seniors) "A Swollen Cell Phone Battery." We also watched Ray Baxter's "Music in the Car." ☺

In Search of a Car Cell Phone Holder

By Joe Nuvolini, P*PCompAS



For some time, I have been searching for the “perfect” car cell phone holder for my 2019 Ford Fiesta. In the photo below are some of the holders I have tried (coffee cup holder, windshield suction, cigarette lighter, and air vent).

Last month’s presentation showing how to hook up various devices and combinations of devices to play media in your car led me to the perfect cell phone holder for my car. It is the one that is inserted into your CD player (if you have one).

After the presentation, I did a Google search for cell phone CD mounts. The one I selected was the MPOW Grip Pro 2.

I bought it on Amazon for $12.99 plus shipping and tax. It is easier to find on the Walmart site and it is $13.99 there. There were several more a little pricier but the MPOW turned out to work just fine. You can see it installed in the photo below (right). You can also view a YouTube video describing it using this link: https://www.youtube.com/watch?v=Ocz5pPV9imA.

Most of the other holders I tried had an arm of some kind and they tend to jiggle a bit when you are on a less than smooth road. In conclusion, the MPOW is rock solid and does not obscure my screen or the controls on the console.

P.S. The unused devices will be available at the “freebie” table at next month’s meeting! ☺

Cryptocurrency (Continued from page 3)

complicated piece of technology, but it boils down to being an online ledger that anybody can view, but not everybody can edit.

Much like the ledger that an old-school accountant would keep (that book Ebenezer Scrooge is hunched over is a ledger, for example), the blockchain records how many there are of any given cryptocurrency and who owns and spends them. It does so in so-called blocks, hence the name “blockchain.” Below is one example of a ledger in action.

4b2fe023d2322e8d2d99970e4582de10a0063cfdcf1a905ff72f7c76efbc23b5	09:24	0.04909712 BTC	$2,235.00
a84301fcfe8ce105112d6feceb2912b408dd93c56056a5343d149c02f88e1addad	09:24	0.00386750 BTC	$176.06
f603276d1458877fa4dcaaa217d6fdf48a4dfb2284700ade5bc65b3e7c6d19612	09:24	1.26709773 BTC	$58,591.46
7770a17c9d9136d8dd17c1880d4159bc970f8aa45d5eef23a53cb32efdf31292ba	09:24	0.00833646 BTC	$379.49
335975a8c3cd48bbd359dda9ef8ef07fe07fe6b12d8e9982d2217c0d733322f74	09:24	0.01198623 BTC	$545.64
f5786046c397c98c090b4430680b64c4eefb4265881dd886784b683cb537ef18	09:24	0.16584376 BTC	$7,549.56
1b41ae9bbeacc1b6337462b127d2c2e7e03fbb131ddbd7bb04598a16b3ea50a3	09:24	0.37840072 BTC	$17,225.60
0db6ab9c69820b848715c78e60c6c40077649d020868debf920852210e2cc30c9f	09:24	0.01296934 BTC	$590.39
ac5dec35ce4ba0fb4bcf84644bf0b68638e63d8671a5092dd3e8d1cb02605e25	09:24	0.00317040 BTC	$144.32
8c5a0f2e10e3fd6fe6e8e2f21f92bf29d9b58c512add21918711e5f92c8b5901	09:24	0.66629159 BTC	$30,331.00

The ledger keeps track of how much of any given cryptocurrency is spent (Bitcoin in the above example), when it’s spent, and also who spent it. Though your identity is protected by a pseudonym—random numbers and letters called a hash—when using most cryptocurrencies, none except for a few exceptions are truly anonymous. Even Bitcoin isn’t “anonymous” in the way many people think it is.

RELATED: *How Anonymous Is Bitcoin?*

Putting the Crypto in Cryptocurrency

The ledger is only one side of the equation. While it’s very nice to have a record of the cryptocoins going in or out, ledgers can be easily tampered with. In the old days, you’d use an eraser or some white-out to make expenses disappear, now you can do much the same with some advanced tools.

One way to guard against these issues is the openness of blockchain technology: if everybody can see what’s going on at any time, it should be

Continued on page 5

Cryptocurrency (Continued from page 4)

easy to quickly figure out if something hinky is going on. The other way is to harness the power of cryptography, or encoding the data of entries and then decoding them as needed.

In the case of cryptocurrencies, this is usually done by using passwords to make sure a user is who they say they are, or rather that their wallet—where cryptocurrencies are stored—is the one that belongs to them. Since the username of a wallet is usually hashed, as we saw before, it's important to make sure that users remember their passwords.

There are several examples of people forgetting their passwords and locking themselves out of their cryptofortune.

Buying and Mining Cryptocurrencies

With the theory of cryptocurrencies out of the way, let's take a look at how they work in practice. To get started with cryptocurrencies, you're going to have to go to an exchange like Coinbase or Kraken to buy your cryptocurrency of choice using regular money. We have a guide on how to buy Bitcoin if you'd like to know more; the guide also applies to other cryptocurrencies.

There are other ways to get your hand on most cryptocurrencies, namely through what's called mining. This isn't anything like swinging a pickaxe, though: instead, a computer is verifying whether new blocks of existing cryptocurrencies are real or fake. Payment for this service is then in that same currency. It's the only way to release new units of a cryptocurrency and thus the best way to get more of it.

However, considering the insane amount of computing power that's needed to process the data necessary for verifying the new blocks, there's a chance your custom-built gaming rig will have smoke billowing out of it before you mine even the equivalent of a few bucks. There's so much processing power needed, in fact, that mining is no longer the field of enthusiasts, but rather of whole companies. Even criminal gangs are getting in on the action—and making millions.

Storing and Spending Bitcoin

Assuming you just bought your cryptocurrency of choice, you still need a place to store it: unlike cash money, Bitcoin and Ethereum can't be sewn into your mattress. For this, you'll need a wallet. These come in software and hardware form and can store your particular blockchain information for you.

A software wallet is often offered by exchanges—though you can subscribe to a separate one, the Bitcoin site has a selection—and is simply an online service where Bitcoin can be stored. Many of them have good security, though they have been falling prey to hackers more and more often.

The alternative is a hardware wallet, which is pretty much just a special USB stick that keeps track of the blockchain for you. Examples include Trezor and Ledger. They're pretty nifty, though again, if you lose or forget your password your crypto is gone.

Once you've settled on a wallet, then all you really need to do is decide what to spend it on. Many online services will let you pay in cryptocurrency, and doing so is pretty easy: just click the right buttons and you should be okay. Alternatively, you could just let it sit in your wallet and watch as the price of it goes higher and higher (or plummets completely). ☺

How Do Websites Keep Passwords Secure?

What to look for in every data breach report

By Leo A. Notenboom, https://newsletter.askleo.com; published under the Creative Commons License

A high-level overview of how websites and services should store passwords security, so next time there's a breach you'll know what to look for.

Note: See the end of the article for an update related to the 9/13 Epik data breach.

We often talk about how you and I should keep our passwords secure, most commonly by using a password vault or manager.

But how do websites work? We trust them to do the same: keep our passwords secure from hacking and exposure. How do they do that?

It turns out to be deceptively simple.

When it's done correctly, of course.

In short: Websites should only store what's called a "one-way hash" of your password, not the password itself. The original password cannot be determined from only its hashed value. If a site can tell you your password, they're doing security wrong. When you next hear of a data breach, pay attention to whether the password information is hashed or not. If it wasn't hashed, that implies your password, if included, is out there for anyone to see.

Websites shouldn't store your password

We'll start with the counterintuitive magic: websites shouldn't store your password. Period.

That leads to the question: how do they know you've entered your password correctly if they don't store it somewhere?

What websites should store is called a "one-way hash" of your password. A hash is a complex calculation that generates a large number. A good hash has three very important characteristics:

- It is statistically impossible for two passwords to generate the same hash number.
- You can create a hash from a password, but *you cannot recover the password from the hash*.
- A small change in the password generates a large change in the resulting hash number, making it impossible to recover "nearby" passwords, even if you know the password/hash combination for some.

That second one is key.

Let's look at an example. I'll use everyone's favorite password: "password".

One hash for "password" is 126,680,608,771,750,945,340,162,210,354,335,764,377. (More commonly expressed in base-16 numbers, aka hexadecimal, as in 5f4dcc3b5aa765d61d8327deb882cf99).

So, if you take *password* and hash it, you'll get 126,680,608,771,750,945,340,162,210,354,335,764,377.

If you hack a database and get that hash, all you have is 126,680,608,771,750,945,340,162,210,354,335,764,377 — you know nothing. There's no way to take that number by itself and determine what password generated it.

Typing the right password

When you set up or change your password, the site you're setting it with will calculate the hash and store that number. If you enter "password" as your password, then our example site will store "126,680,608,771,750,945,340,162,210,354,335,764,377" in its database, along with your user ID and/or email address.

Now, days or weeks later you come back to the site and sign in. Here's what happens:

- You enter your password ("password", in our example).
- The site calculates the hash (126,680,608,771,750,945,340,162,210,354,335,764,377 in our example).
- The site compares the hash it just calculated against the hash it stored when you set your password.
    - If they match, you must have typed your password correctly, since only the exact same password would

Continued on page 7

Website Breaches (Cont. from page 6)

generate the exact same hash.
- If they don't match, you didn't type the expected password that goes with the expected hash.

That's really all there is to it. Aside from some complex math to generate the hash, it's pretty simple.

Telling you your password

I repeatedly used the word "should" above.

A website doing password security correctly should only store the password hash, not the actual password. Since there's no way to go backward — recovering the password from the hash — that means *a website using proper security cannot tell you what your password is*. They can only tell you that you typed it correctly or not.

Unfortunately, not all sites do security correctly, and there's at least one way to test:

If a website can tell you your password, then they've got that password stored as-is in a database the staff can access.

That's poor security because your password could be exposed in a breach.

Passwords and data breaches

The next time you hear of a large data breach, particularly if it's happened at some online service you use, pay careful attention to the wording describing the information that was exposed.

For example, here's a description of a recent breach from HaveIBeenPwned:

*In June 2020, the restaurant solutions provider OrderSnapp suffered a data breach which exposed 1.3M unique email addresses. Impacted data also included names, phone numbers, dates of birth and **passwords stored as bcrypt hashes**. The data was provided to HIBP by dehashed.com.*

(Emphasis mine.) The passwords were stored as hashes. In this breach, passwords were not exposed. While there was other information included in the hack, the most sensitive of all — passwords — had been stored correctly.

Contrast that with this description:

*In January 2019, a large collection of credential stuffing lists (combinations of email addresses and passwords used to hijack accounts on other services) was discovered being distributed on a popular hacking forum. The data contained almost 2.7 billion records including 773 million unique email addresses alongside **passwords those addresses had used** on other breached services.*

There's no mention of hashing at all. This particular breach included actual passwords. Wherever those passwords came from, there was a lapse in security of some sort.

This is what you pay attention to: were the passwords exposed in a breach hashed? If not, change your password on the impacted service *immediately*. If they were hashed, you can still change your password if you like — and perhaps you should for other reasons — but you can be somewhat less concerned that your password is "out in the wild."

There's more to security than passwords

It's important to note that of course, there's much more to website security than whether or not passwords are hashed. Let's face it: data breaches shouldn't happen, either, but they do.

Hashing is just one (very important) part of website and online service security, which encompasses everything from keeping the web servers themselves secure and malware-free, to using proper database and software security, to ensuring only the proper personnel have access to sensitive information.

It's a complex world, and easy to get wrong, as every breach we hear about reminds us.

But the next time you hear of yet another breach, now you'll have at least one thing to look at to determine just how security-conscious the service was and how worried you should be.

A quick note to pedants

Since this type of overview tends to bring out those with an eye for excruciating detail and minutia, one small caveat:

This is only a high-level overview to make the concepts accessible to more people. Of course, password management implementation details can get very complex. If you're about to comment with a complaint that I didn't discuss different hashing algorithms (ugh), or that MD5 shouldn't be used for passwords (I agree), or that password hashes should be salted (ditto), and why didn't I talk about rainbow tables (hoo, boy) . . . don't.

Those concepts were never the point.

Continued on page 8

Free Programs to Keep Your Computer Software Up To Date

by Serena O'Sullivan at Komando.com (article from 6/16/21)

Developers are always working hard to improve the software on your computer. That's because hackers are always analyzing popular programs for bugs and hidden backdoors. When they find an opening, the news spreads like wildfire — and then it's open season on your digital life.

Because of this, keeping your programs updated is one of the most effective ways to protect yourself from hackers. But it can be hard to stay on top of all the programs. After all, who wants to check for software patches and operating system flaws manually?

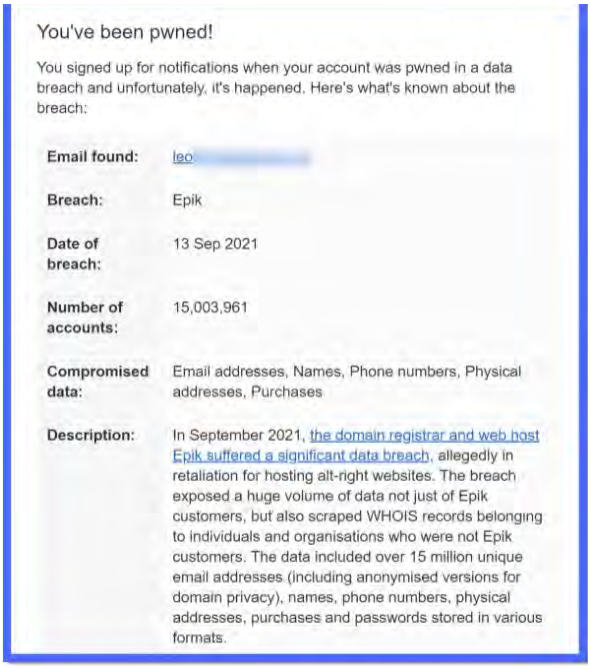
It can seem like a daunting task. Luckily, you don't have to worry about working hard to protect

Continued on page 9

Website Breaches (Cont. from page 7)

Update 2021-09-19: an example breach

On September 19th, 2021 Have I Been Pwned sent notifications to registered users involved in the so-called "Epik" data breach.



You've been pwned!

You signed up for notifications when your account was pwned in a data breach and unfortunately, it's happened. Here's what's known about the breach:

Email found:	leo
Breach:	Epik
Date of breach:	13 Sep 2021
Number of accounts:	15,003,961
Compromised data:	Email addresses, Names, Phone numbers, Physical addresses, Purchases
Description:	In September 2021, the domain registrar and web host Epik suffered a significant data breach, allegedly in retaliation for hosting alt-right websites. The breach exposed a huge volume of data not just of Epik customers, but also scraped WHOIS records belonging to individuals and organisations who were not Epik customers. The data included over 15 million unique email addresses (including anonymised versions for domain privacy), names, phone numbers, physical addresses, purchases and passwords stored in various formats.

The notification does indeed talk about passwords, specifically "passwords stored in various formats." Unfortunately, that's not a lot to go on and tells you nothing about how concerned you should be.

If you are an actual Epik customer, assume the worst and change your password immediately. Also, if you're using that same password anywhere else, change it in all the places you've used it. Take this opportunity to stop re-using passwords and set them all to something unique.

The scraped "WHOIS records" will not include passwords. This is already generally public information about who owns domains on the internet; for example, it'll tell you I own askleo.com. Nothing particularly alarming here.

But what about . . . anything else? It *seems* that only passwords of Epik customers were exposed (in various formats), but there's no indication of any other account-related information we need to be concerned about.

But, as always, it pays to remain watchful for unexpected activity on your accounts.

RELATED QUESTIONS

Can a website owner see my password?

Website owners can possibly view your password in either of two ways. One, they can watch your keystrokes as you type in the password when signing in to their site; or, if they actually store your password in plain text in their database, they can also view it there. Note that the latter is considered bad security since anyone with access to the database would be able to view your password.

Where can I keep all my passwords safe?

The best way to keep all of your passwords safe is to use a password vault. These utilities store your passwords securely encrypted and accessible only to you. Many include additional features, such as automatic password entry, password generation, and in some cases, notification if an account is compromised or if a password you're using is not secure for any reason. ☺

Software Up to Date (Cont. from page 8)

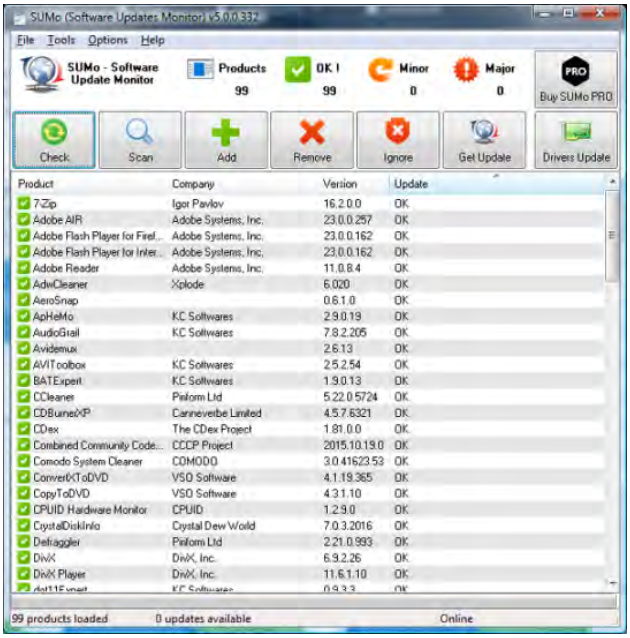
yourself. These free tools can update your outdated software, taking all the heavy lifting off your hands. Here's how you can protect your computer.

A software updater is like a digital bodyguard: it tells you about outdated software so you aren't taken by surprise

One of our favorite programs is SUMo, which stands for "Software Update Monitor." This free app lets you know when programs on your PC need extra attention.

It automatically spots required updates and patches for your software, and it knows when new drivers are ready for download. It's also versatile in that it can check apps as well as screensavers and other add-ons. Basically, it ensures that your whole system is always up-to-date.

It's handy since it distinguishes between the types of updates your app needs. For example, it'll recognize a major update compared to a minor update, which gives you the power of choice. Plus, you can run it from a portable location if you're on the go.

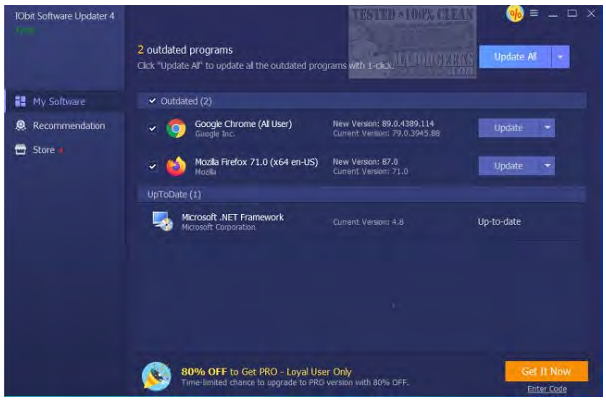


All you need to do is run the app and give it time to complete its scan. Once done, it will provide you with a list of all your missing updates, which you can browse through to decide which you want to download.
http://www.kcsoftwares.com/?sumo

Not sure you want to get in the ring with SUMo? Here's another free software updater that can wrestle away outdated programs: **IObit Software Updater**.

This program wears many hats. Not only is it simple and easy to use, but it's stuffed with helpful features, like bulk downloading and updating as well as in-program updates.

Plus, its interface is crisp, revealing current and new version numbers. So you know exactly what you're working with. The only shortcoming we could find: You have to pay if you want automatic updates. ☺



Tip: How to Change the Lock Screen Photo on Windows 10

Here is how to change the default photos on the lock screen:

1. Click Settings (the gear icon).
2. Click Personalization.
3. Click on "Lock Screen."
4. Click on the drop-down menu under "Background" and scroll to "Pictures." You can choose to show an individual picture, a slideshow, or the default Windows spotlight.
5. Choose one of the pictures that pops up or hit "Browse" to select a picture from your library. Make sure that the picture you want is located in the far left of picture lineup.

P*PCompAS Newsletter
Greg Lenihan, Editor
4905 Ramblewood Drive
Colorado Springs, CO 80920
e-mail: glenihan@comcast.net

Coming Events:
Next Membership Meeting: 2 October beginning at 9 am (see directions below)
Next Breakfast Meeting: 16 October@ 8:30 am, Perkins, 3295 E. Platte Ave.
Newsletter Deadline: 23 October
Check out our Web page at: http://ppcompas.apcug.org