BUSINESS

Alexander: How to change your iPhone's photo format to print pictures

Since 2017, Apple has let users choose their photo formats inside iPhone.

By Steve Alexander Special to the Star Tribune

SEPTEMBER 12, 2021 — 2:00PM

The photo format in iPhones has to be changed to work with commercial printing services.

Q: I haven't been able to send my iPhone photos to Walgreens and Walmart for printing due to a format issue — the photos were in the HEIC (High Efficiency Image Coding)file format the iPhone uses. I then saved the photos in the JPEG (Joint Photographic Experts Group) file format the stores wanted, but I was told that some JPEG photos also aren't accepted. What can I do? THOMAS ELWOOD, Bedford, N.H.

A: The photo printing services of Walmart and Walgreens require you to send them photos in the JPEG (also written as JPG) file format, which is widely used by digital cameras. The main restrictions are that Walmart won't accept any photo larger than 16 megabytes (see tinyurl.com/4ne5w4ha), and Walgreens discourages sending a photo larger than 20 megabytes (see tinyurl.com/pez3kt25). These limitations probably won't affect you; iPhone JPEG photos typically contain less than 10 megabytes of data.

The HEIC photo format (Apple's version of the standard HEIF, or High Efficiency Image Format) was designed to save storage space on iPhones. HEIC photos require only about one-third as much storage space as JPEG photos. The drawback to HEIC is that some photo-printing services and non-Apple devices don't use that format. So, since 2017 Apple has let you choose which format your iPhone should use for photos. To pick one, go to Settings, click on camera, then click Formats. Choose "high efficiency" for HEIC or "most compatible" for JPEG.

If you've already taken a lot of photos using HEIC, there are plenty of programs that can convert them to JPEG (see tinyurl.com/f3tkzd or tinyurl.com/373buv84). In addition, online file storage services such as Dropbox and Microsoft OneDrive can convert your HEIC photos to JPEG format when you upload the pictures from your iPhone.

Q: Until now, whenever I used my wireless mouse with my HP laptop, the PC's touchpad became inactive. But now the touchpad will not turn off, and this PC doesn't seem to have an

enable-disable control for it. I've tried all the suggestions I could find online, but nothing works. What can I do?

PATRICIA TRAPP, Glastonbury, Conn.

A: It is possible to disconnect the touchpad. But first you need to make sure that your mouse is working properly. Otherwise, you could wind up with no way to access your PC.
Try reconnecting the wireless mouse to your PC to make sure it's set up correctly (you can search Google for step-by-step directions for your mouse's brand and model.) If for some reason the mouse won't connect, check to see if the mouse itself has been "disabled" on your PC.

To do that, use the touchpad to open Control Panel and click on "device manager." You'll get a list of all the devices on your PC. Scroll down to "mice and other pointing devices" and click on it. You should see two devices listed: Your mouse and something called "input device," which is your touchpad. Click on the mouse, and at the top of the resulting menu click the "driver" tab. Make sure that the mouse is "enabled" (if you're given a choice to disable the mouse, then it is enabled.) If the mouse still doesn't connect properly, there's something wrong with it.

Once you know the mouse is working properly, go back to device manager, click on "mice and other pointing devices" and this time click on "input device." At the top of the resulting menu, click the "driver" tab. Click on "disable device," then click OK.

E-mail tech questions to steve.j.alexander@gmail.com or write Tech Q&A, 650 3rd Av. S., Suite 1300, Minneapolis, MN 55488. Include name, city and telephone number.

BUSINESS

Alexander: Protection against 'brute force' and 'dictionary' attacks

Here's what hackers do to get past password attempt limits, and what you can do to safeguard your computer.

By **Steve Alexander** Special to the Star Tribune

SEPTEMBER 26, 2021 — 2:00PM

There are ways to protect your home computer against “brute force” and “dictionary” attacks.

PRINT
MORE

Q: Many password-protected websites give you a few chances to type in your password correctly, then lock you out if you type the wrong thing. You then must type in a code or answer a "secret question" to prove who you are.

So why do I see TV shows in which smart criminals use a computer to test, say, 10,000 passwords a minute until they get the right one to break into a website? Why aren't the criminals locked out after a few wrong passwords?

JERRY ROVENTINI, Lakeland, Fla.

A: The TV shows are less far-fetched than you might think.

The scenario you're describing is called a "brute force" attack. A computer connects to a web server and rapidly tries a long list of possible passwords until it hits the right one. A real brute force attack would require about two hours to crack an eight-character password composed of letters (upper and lower case), numbers and special characters (see tinyurl.com/4r2debx3).

How would the attackers avoid being locked out during those two hours? Sophisticated hackers could disable the server's "intrusion detection system," or its automatic "password attempt limit" (which normally locks a person out after a few wrong tries).

But because brute force attacks require some expertise, they're less common than a simpler threat called a "dictionary attack." The "dictionary" is a short list of common passwords that a computer can try in much less than two hours. These attacks succeed when people use simple passwords, such as "password" and "123456," which take fractions of a second to crack.

While it's hard to believe that people still use such vulnerable passwords, here's an interesting fact: The 2019 attack on Texas IT company SolarWinds, a federal contractor, revealed that an employee used the password "solarwinds123" to access a server. A Congressional investigation

criticized the use of such simple passwords, but the company determined the password was not the vehicle of the attack.

And, based on information from other data breaches, here's a list of the most common passwords of 2020, how often they were hacked and how little time it took (see tinyurl.com/zu2ekpdt). The password list includes "abc123," "111111" and "iloveyou."

There are ways to protect your home computer against “brute force” and “dictionary” attacks.
TEXT SIZE

Q: Many password-protected websites give you a few chances to type in your password correctly, then lock you out if you type the wrong thing. You then must type in a code or answer a "secret question" to prove who you are.
So why do I see TV shows in which smart criminals use a computer to test, say, 10,000 passwords a minute until they get the right one to break into a website? Why aren't the criminals locked out after a few wrong passwords?

JERRY ROVENTINI, Lakeland, Fla.

A: The TV shows are less far-fetched than you might think.
The scenario you're describing is called a "brute force" attack. A computer connects to a web server and rapidly tries a long list of possible passwords until it hits the right one. A real brute force attack would require about two hours to crack an eight-character password composed of letters (upper and lower case), numbers and special characters (see tinyurl.com/4r2debx3).
How would the attackers avoid being locked out during those two hours? Sophisticated hackers could disable the server's "intrusion detection system," or its automatic "password attempt limit" (which normally locks a person out after a few wrong tries).

But because brute force attacks require some expertise, they're less common than a simpler threat called a "dictionary attack." The "dictionary" is a short list of common passwords that a computer can try in much less than two hours. These attacks succeed when people use simple passwords, such as "password" and "123456," which take fractions of a second to crack.

While it's hard to believe that people still use such vulnerable passwords, here's an interesting fact: The 2019 attack on Texas IT company SolarWinds, a federal contractor, revealed that an employee used the password "solarwinds123" to access a server. A Congressional investigation criticized the use of such simple passwords, but the company determined the password was not the vehicle of the attack.

And, based on information from other data breaches, here's a list of the most common passwords of 2020, how often they were hacked and how little time it took (see tinyurl.com/zu2ekpdt). The password list includes "abc123," "111111" and "iloveyou."

The best defense against brute force and dictionary attacks is to use a password that is a long combination of letters, numbers and symbols that would be meaningless to anyone but you. These so-called "nonpredictable passwords" are far more difficult to hack.

Q: I keep getting a Windows 10 message that's supposed to be from Microsoft — but I wonder if it's a scam. It reads: "We need to fix your Microsoft account (most likely your password changed). Select here to fix it in shared experiences settings." Are you familiar with this? PIERRE GIRARD, Golden Valley

A: It's a legitimate Microsoft warning, but it's being triggered by a Windows 10 error. Several fixes have been suggested:

- Disable your PC's "share across devices" feature, which makes it easy to exchange data with other computers and phones. (See the "settings app" method at tinyurl.com/3dknadj3.)
- If you are logging into Windows 10 with your online Microsoft account password, switch to a "local" account that doesn't depend on your online identity (see tinyurl.com/act82bu4).
- Make sure your PC is a "trusted device" that's listed in your Microsoft account (see tinyurl.com/sykz6wzk).

E-mail tech questions to steve.j.alexander@gmail.com or writer to Tech Q&A, 650 3rd Av. S., Suite 1300, Minneapolis, MN 55488. Include name, city and telephone number.

BUSINESS

Work needed to make electric vehicles a jobs powerhouse in U.S.

Report says subsidies may be needed to make sure jobs are not lost in the transition away from gasoline-powered cars.

By Noam Scheiber New York Times

SEPTEMBER 26, 2021 — 2:00PM

An electric vehicle charging station in California's Bay Area. Government subsidies might be needed to avoid job losses in auto manufacturing.

MORE

When President Joe Biden announced his multitrillion-dollar jobs plan in March, it included nearly $175 billion in spending to encourage Americans to buy electric vehicles.

The money would help ensure "that these vehicles are affordable for all families and manufactured by workers with good jobs," the White House wrote at the time.

Now, as Biden's plan wends its way through Congress, a liberal think tank has tried to flesh out the number of jobs to be gained or lost in the transition away from internal-combustion vehicles.

The report, released Wednesday by the Economic Policy Institute, concluded that it would take government subsidies focused on developing a domestic supply chain and increasing demand for U.S.-made vehicles to avoid job losses.

It found that without additional government investment, the industry could lose about 75,000 jobs by 2030, the year by which Biden wants half the new vehicles sold in the country to be electric.

By contrast, the report said, if government subsidies were targeted to increase the portion of electric vehicle components that are manufactured domestically, and to increase the market share of U.S.-made vehicles, the industry could add about 150,000 jobs by the end of the decade.

"That's the payoff — making the sector a center of good jobs again," said Josh Bivens, an economist who is one of the report's authors. "If we don't try to react proactively with good policy we'll see continued downward pressure on the number of good jobs."

Looming over the transition to electric vehicles is the fact that they have substantially fewer moving parts than gasoline-powered ones and require less labor to manufacture — about 30% less, according to figures from Ford Motor. The vehicle-manufacturing industry employs a little under 1 million people domestically, including suppliers.

There are essentially two ways to offset the projected job losses: to increase the proportion of each vehicle's parts that are made domestically — specifically in the powertrain, the key parts and systems that power a car — and to sell more vehicles assembled in the United States.

Bivens and his co-author, James Barrett, an economic consultant, examine the effects of doing both. They note that roughly three-quarters of the parts in the powertrain for a U.S.-made gasoline vehicle are produced domestically vs. less than half the parts in the powertrain of a U.S.-made electric vehicle.

Raising the proportion of domestic content in electric vehicles so that it mirrors gas-powered ones could save tens of thousands of jobs a year, they estimate — potentially more than half the likely job losses that would arise without additional government action.

But to transform likely job deficits into job gains, Barrett and Bivens find, it is necessary to increase the market share of U.S.-made vehicles. According to the study, the percentage of vehicles sold in the United States that are made domestically has hovered around 50% over the

past decade. If it were to rise to 60%, the authors conclude, the industry could gain more than 100,000 jobs in 2030.

If market share were instead to drop to 40% by the end of the decade and there were no increase in the domestic content of electric vehicle powertrains, the industry could lose more than 200,000 jobs, the report finds.

Under the Democratic plan circulating in Congress, a current $7,500 tax credit for the purchase of a new electric vehicle would rise as high as $12,500. An extra $4,500 would apply to vehicles assembled at unionized U.S. factories. Consumers would receive the final $500 if their vehicle had a U.S.-made battery. The details could change in the face of opposition from automakers with nonunion U.S. plants.

Democrats are also discussing subsidies to encourage manufacturers to set up new factories or upgrade old ones.

Sam Abuelsamid, an auto industry analyst at Guidehouse Insights, said that domestic automakers had an opportunity to increase market share as the industry electrifies and that an expanded consumer tax credit would help.

"They are targeting a lot of the market segments that are particularly strong-selling — crossovers, pickups," Abuelsamid said. "There is definitely potential for them to claw back some market share from Asian brands."

Still, he warned, the window for seizing the opportunity could be relatively narrow as Asian automakers like Toyota and Honda, which have lagged somewhat in their electric vehicle planning, introduce more electric offerings.

The question of whether manufacturers will locate production of electric vehicles and their components in the United States as demand grows, and the extent to which government subsidies can help ensure that this happens, has been a subject of debate in recent years.

Dale Hall, a researcher at the International Council on Clean Transportation, a research organization, said that electric vehicles tend to be manufactured in the region where they are sold, both to save on transportation costs and to be more responsive to consumers' needs.

But his group has found that there is nonetheless variation among regions: About 98% of electric vehicles sold in China last year were assembled in that country, while 72% of those sold in the United States were assembled domestically. One key difference is government policy.

"China provided a lot of subsidies to manufacturers in the early days," Hall said.