

HOW TO CREATE DESKTOP SHORTCUT TO FAVORITES IN WINDOWS 10

Creating a Desktop shortcut enables Windows 10 users to quickly access items of daily use. You can also add your **Favorite** items to the Desktop as shortcuts. So, if you are interested in creating a **Desktop Shortcut to Favorites** in Windows 10, here's how it is done.

In Windows 10, the File Explorer favorites are seen pinned under Quick Access in the left side of File Explorer. You can choose to keep the Desktop screen as the default location of your favorites. For this, you'll need to do the following things.

1. Right-click on your Desktop
 2. Select New > Shortcut
 3. Paste the Favorites string value in the Target box
 4. Name the shortcut
 5. Customize the icon.
- The Favorites folder you are trying to create can include shortcut links to either Desktop, Downloads, or your favorite apps. Now let us see the procedure in details.

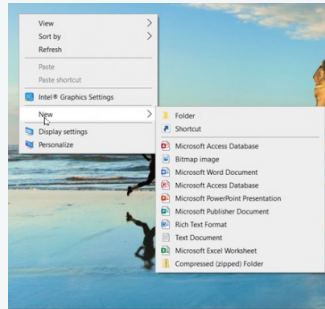
(continue)



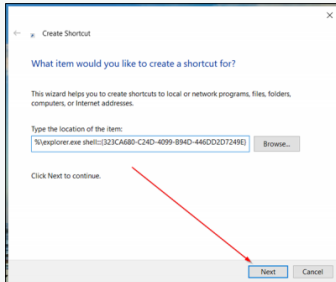
103 E. Poplar
Greencastle, IN 46135
765-653-2755
www.pcpl21.org

(continued)

1] Create and name the shortcut

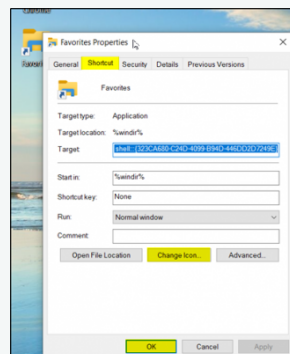


To create a Desktop shortcut, right-click anywhere on your Desktop screen and select New > Shortcut.



Next, paste the following text in the location of the item and hit 'Next' button.

```
%windir%\explorer.exe shell:::  
{323CA680-C24D-4099-B94D-  
446DD2D7249E}
```



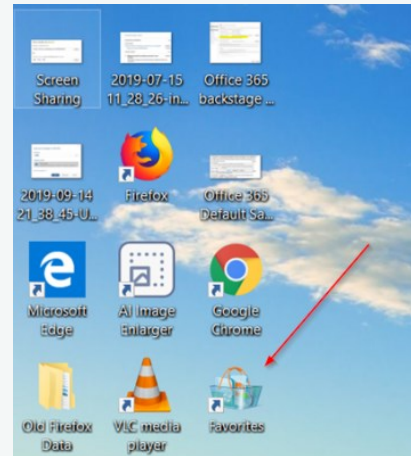
(continue)

(continued)

When done, name the new shortcut as 'Favorites' and click Finish.

If you would like to change the shortcut icon to something you like, then, right-click on it and select 'Properties'.

In the 'Fav Properties' window that opens on your computer screen, switch to 'Shortcut' tab, and hit the 'Change Icon' button.




After that, simply select an icon you want to use or browse to the location of a custom icon and click OK.

That's it! The Desktop Shortcut to Favorites will be created and seen on the screen.

If you would like to pin it to the Taskbar, simply right click the icon and choose 'Pin to taskbar'.

End


**Community Help
Desk Hours**
Monday
4:00 to 7:30
Tuesday
1:00 to 4:00
Wednesday
1:00 to 7:30

(There will be no help desk on Thursday or Friday)

WINDOWS PHONE IS DEAD! WHAT IS NEXT FOR WINDOWS 10 MOBILE USERS?

Despite a series of acquisitions (Nokia) and tie-ups (Samsung), Windows Phones weren't as profitable for Microsoft as planned, and thus the company stopped manufacturing and focusing on them. The major cause for its failure can be attributed to the lack of quality apps. However, the support continued for the devices, until Microsoft ceased support for Windows 8.1 Mobile in 2017.

In a recent announcement, the IT giant has now clarified that the support for Windows 10 Mobile would end as of December 10, 2019. This means Windows 10 Mobile users would not receive any updates or any assistance at all from Microsoft.

Why is Microsoft ending support for Windows 10 Mobile?

Technology has evolved along with the needs and expectations of your customers and partners who have already adopted Android or iOS platforms and devices. Microsoft's mission statement to empower every person and every organization on the planet to achieve more compels us to support our Mobile apps on the supported Android and iOS devices.

What about the app support on Windows Mobile devices?

Both Microsoft and third-party apps on Windows Mobile devices have a different support system and are separate from the general operating system support. This makes sense because the same apps could be compatible with your PC, Xbox, or Hololens device.

Thus the apps would be supported by their provider the way it was intended to be and has nothing to do with this announcement in particular.

Can users use Windows Mobile devices after 10th December 2019?

Why not! While Microsoft is ramping down the support for its mobile devices, it doesn't shut down the device itself.

(continue)

(continued)

Users could continue using their Windows Mobile devices. However, since Microsoft wouldn't roll out any security updates, you would need to understand that you would be using the device at your own risk.

What should Windows Mobile users do on such a situation?

It needs to be understood that Microsoft stopped manufacturing mobile devices quite some time ago and the current situation was anticipated. Thus, if you have a Windows Mobile device, you could consider buying a new Android or iOS mobile device.

If you wish to continue using your old Windows Mobile device, it would be advisable to backup your phone. To back up the data of a Windows 10 Mobile device, go to the following location Settings > Update & security > Backup > More Options. Select *Back up now*.

Will the phone work after December 10, 2019?

Yes. The Windows 10 Mobile device should continue to work after December 10, 2019, but there will be no updates after that date, and device backup functionality and other backend services will be phased out.



For more tips and tricks visit: <https://www.thewindowsclub.com/>

Exceptions

No Windows mobile device is an exception to this announcement, even if they were procured commercially. However, this announcement is for devices running on Windows update 1709. Support would cease for devices running on 1703 on June 11th, 2019.

For more information, please check the reference on Microsoft's Support website. (END)

HOW TO DETECT AND AVOID PAYPAL SCAMS

Whether you want to kick-start an online business or want to do safe online shopping, PayPal unquestionably is one of the most secure and convenient platforms. Since its inception, PayPal has endured being the de-facto ways to send/receive money online. Although PayPal is a very dependable service, scammers still manage to spot the loopholes and escape roads to dodge PayPal's anti-scam defenses using cheap tricks.

Let's face it, PayPal scams do occur, and scammers ought to trick you if you regularly use this platform for online transactions. With this blog, we aim to bring into your notice a few ways scammers cheat people on PayPal and how you can avoid PayPal scams.



HOW TO DETECT AND AVOID PAYPAL SCAMS



Avoid PayPal Scams

Criminals are obstinate, but you can avoid falling into their scam traps by being proactive and knowing what to watch out for. Be aware of these most common PayPal scams.

1. Advance Fee Fraud
2. Email Scam
3. Display Name Spoofing
4. Fake Charities
5. Overpayment Scam
6. Shipping Scams
7. Employment Scam.

Let's look at all these PayPal scams in detail:

1] Advance Fee Fraud:

As humans, we are very cautious about strangers on the street, sadly in the online world, we aren't that cautious. One of the most common PayPal scam users should be cagy of is 'Advanced Fee Fraud'. Here fraudsters will request you to send some smaller amount (for legal documentation, taxes, etc.) before they can transfer your millions – The truth, these irresistible offers are scams.

Here you may receive an email with a subject line in ALL CAPS claiming you've won a legacy. When you open such emails, you may find an official letter from someone in a high political position telling you that you're due to an insane amount of money for some phishing reason. What happens next? You are asked to provide some basic information which explicitly opens up the lines of communication. Ultimately, the scam successfully collects your personal information can be used in identity fraud, while also grifting money from victims.

(continue)

(continued)

How to avoid – Don't rope money to someone you don't know. A legitimate prize won't require you to pay a sum to receive it.

2] Email Scam – “Your Account Is About To Be Suspended” Or “Problem With Your Account”:

Another PayPal scam comes in the form of emails; many scammers send hoaxed emails warning indicating an account is about to be suspended, or there is some issue with the account. The account holder is tricked into opening the email and clicking on a link which directs them to a phishing website. Furthermore, the victim should enter their PayPal account password in the spoofed webpage.

How to avoid – PayPal is never going to ask you to enter your login details unless you on their login page. Report any suspect email by forwarding it straight to spoof@paypal.com. Also, it's a good idea to change your password frequently.

3] Display Name Spoofing:

Also known as “friendly name” scams, fraudsters utilize a feature of the email systems which lets the sender's display name to hide behind a “friendly name”, this makes it look very genuine. Cheats can easily fake the “friendly name” in the sender's email address. For example, an email can look like coming from “PayPal Services,” but be from sqz7@twomail.com.

How to avoid – Open the suspected email, but NEVER click any links in the email. Also, hovering over the display name in the email will display the real email address so you get to know if its hoax.

(continue)

(continued)

4] Fake Charities:

Fraudsters tend to play with victims' emotions too; in a few cases, these can include tricking kind-hearted people into donating to bogus charities. Many fake charities pop up from nowhere following occasions of a refugee crisis, a terrorist attack or a natural disaster (like an earthquake, flooding or famine). In such fraud events, these charities may have a fake website, or they simply send information over the web – ultimately ask victims to pay through their PayPal accounts.

How to avoid – Before making any donations, check the background of the charity. For verifying charities, PayPal itself recommends using one of the following websites:

- <http://www.charitynavigator.org>
 - <http://www.bbb.org/us/charity>
 - <http://www.charitywatch.org>
- Note if you cannot verify the charity through any of these options, it is expected to be fake.

5] Overpayment Scam:

PayPal vendors should be concerned about this scam. What happens here?

- The vendor sells a product/service to an individual/business
- The buyer makes a payment but sends more money
- The buyer then requests the vendor to return the difference
- But the catch here is that this time the buyer wants the refund to a different account.

(continue)

HOW TO DETECT AND AVOID PAYPAL SCAMS

(continued)

How to avoid – A legitimate buyer will never overpay you for an order. If a customer overpays you and asks for a refund for the difference, consider canceling the order and do not ship the product. And, never return the money to a different account.

6] Shipping Scams:

The shipping scams occur in two way, service scam and address scam.

- **Shipping Service Scams:**

The buyer can ask you to use a specific shipping service. They can claim that they have a preferred vendor who is more reliable or they can get a discount. In all certainties, they can easily contact the shipping company and reroute the order to another address and later file a complaint about not receiving the item at the original address.

How to avoid: Use only your shipping account and review and validate the buyers' address before shipping the product.

- **Shipping Address Scams:**

Here the scammer tempts you to make a delivery to a different address other than the registered one with PayPal. They will make the payment through their PayPal account, but the item needs to be delivered to a different address. Once the item is delivered, these scammers will open a dispute that they never received the product.

PayPal security guidelines mention clearly that you should never deliver an item to an address other than the one it is registered with on PayPal. This platform takes no responsibility for the delivery of goods which have not been delivered to the address registered with the buyer's PayPal account. Now even if you provide shipping confirmation receipt, PayPal will not do anything about it.

(continue)

(continued)

How to avoid – Never deliver an item to an address other than the one it is registered with on PayPal.

7] Employment Scam:

This occurs when someone offers you to be their partner or employee. They ask you to trade products on eBay or a website, pay their supplier, and update your PayPal account address to their address. Such fraudsters can conduct fraudulent transactions and hold you liable.

How to avoid – First thing, verify such suppliers. Never pay on behalf of someone you don't know and never update your PayPal account address to someone else's.

Detect Fake PayPal Emails

While the above-mentioned PayPal scams are the most common ones, you must know that numerous fake emails are being frequently used to cheat users worldwide. Today there are hundreds of ways fraudsters can use fake emails to cheat people. But following a basic email scam prevention rules can help in the prevention of these dodges. Below are some clues that can help detect fake PayPal email scams:

- An email from PayPal will always come from paypal.com and not support@paypal.com.
- Phishing emails will ask for confidential information, like bank details, PayPal login details, full name, your security question's answer, and other similar information which can be exploited.
- PayPal emails will never contain attachments and will never ask you to install or download anything.

(continue)

(continued)

- PayPal emails will always address you by your first and last names, or your business name.
- Scam email content creates a sense of urgency. For example, "Click now to get \$100 coupon" or "We have noticed wary activity in your account, click the link below to confirm".

Always make sure your email spam filters are turned on, this will automatically put emails from unknown sources into junk/spam folders. Also, when you receive emails from any suspicious emails instantly add them to your block senders list.

Last Words

In the case of fraud, your best option is to contact **PayPal.com** directly. PayPal offers fraud protection for all buyers and sellers who utilize their service. If you believe a mismatch in your transaction or any fraudulent activity, report to PayPal within 60 days. The company will investigate the issue and verify the information.

It is also very important that you keep track of your PayPal account, even if you don't use it that often. Log in securely once a while and check the history of your payments; also make sure you create a very strong password to help secure your account. Even though PayPal is the most trusted payment service on the Internet, there are ways around its security which can lead to a breach.

Now you since you know how these scammers operate and the tricks they use – **Be careful!**

(END)

