

Everyone complains when their Facebook page gets "hacked". It's a pain for everyone but it can also be devastating. The worst and most dangerous Facebook scam is making the rounds again. It often starts with a friend who has their profile cloned. One of our viewers fell victim to this scam and unknowingly sent it to me. How does it work? And what should you do if you get it? I'm looking at how the "do you know this person?" scam and what happens if you click the link.

TRT 138
STD OUT

super:
0-8 Jamey Tucker/whatthetech.tv

On camera tease

Most Facebook scams are just an annoyance, but one making the rounds right now could kill your Facebook account forever. I'm Jamey tucker I'll show you want to watch for, coming up

ANCHOR INTRO

A CONSUMER WARNING FROM MULTIPLE LAW ENFORCEMENT AGENCIES ACROSS THE COUNTRY ABOUT A FACEBOOK SCAM MAKING THE ROUNDS AGAIN THAT CAN STEAL INFORMATION AND EVEN YOUR ENTIRE FACEBOOK ACCOUNT.

PERHAPS YOU'VE SEEN IT, OR EVEN CLICKED ON THE SCAM FREQUENTLY REFERRED TO AS THE "LOOK WHO DIED" SCAM. AS OUR CONSUMER TECHNOLOGY REPORTER JAMEY TUCKER EXPLAINS, THIS SCAM IS DANGEROUS AND CAN TAKE DOWN YOUR ENTIRE FACEBOOK ACCOUNT.

Package script

This Facebook scam is easy to recognize and easy to avoid. Still, people fall for it every day. even smart people. And one of our viewers sent it to me. Only, he didn't know it Here's the scam, posts or messages that say "look who died, I think you know him" followed by several crying emoji. It appears to be a link to a news report.

Here's what happens if you click the link, rather than playing a video, you're prompted to sign in to your Facebook account to see it.

It isn't a Facebook log in though, look at the address. If you enter your username and password, the bad guys can log into your account. They can also change your Facebook password and you won't be able to log back in.

But the posts or messages come from Facebook friends. That's because those friends are among those who have their profiles cloned. It happens thousands of times a day. Pay attention to where a link is going. Not to a news outlet, but to websites with strange names. The posts almost always tags you or some of your friends. They also come through as Facebook messages from friends who've had their Facebook profiles compromised. IF you've clicked on a link and entered your login information. Change your password as quickly as possible and everyone should have 2-factor authentication turned on to make it more difficult for the hackers to change passwords. This scam can spread through email, social media, and text messages. And remember just because it looks like it's coming from someone you know who's pretty smart, it's still a scam. That's What the Tech? I'm Jamey Tucker

ANCHOR TAG

FACEBOOK ASKS USERS TO REPORT ANY SCAMMY POSTS OR MESSAGES AND OF COURSE, NOTIFY THE FRIEND WHO SHARED THE POST THAT THEIR PROFILE HAS BEEN COMPROMISED.

WEB STORY

A Facebook scam that dates back years is making another round of appearances in posts and messages. Law enforcement agencies are alerting Facebook users of what's being referred to as the "Look who died scam".

This Facebook scam is easy to recognize and easy to avoid. Still, people fall for it every day.

Here's the scam: posts or messages that say "Look who died, I think you know him" followed by several crying emojis. It appears to be a link to a news report or YouTube video.

If you click the link, rather than playing a video, you're prompted to sign in to your Facebook account to see it.

It isn't a Facebook log in though. A closer look at where the link goes reveals a strange-sounding website URL. But the login page itself looks legitimate. If you enter your username and password, the bad guys can log into your account. They can also change your Facebook password and you won't be able to log back in.

Though it wasn't the same scam, tens of thousands of Facebook users recently got scammed, had their Facebook profiles hijacked, and everyone's name was changed to Lilly Collins. It took some of the victims weeks to get a response from Facebook.

The posts or messages come from Facebook friends who've had their profiles cloned. It happens thousands of times a day.

The posts almost always tag you or some of your friends. They also come through as Facebook messages from friends who've had their Facebook profiles compromised.

Facebook responds to reports of these scammy posts, but they'll generally stay up for a few days nabbing more victims.

If you've clicked on a link and entered your login information. Change your password as quickly as possible and everyone should have 2-factor authentication turned on to make it more difficult for the hackers to change passwords.

Always be on alert. This scam can spread through email, social media, and text messages. And remember just because it looks like it's coming from someone you know, it's still a dangerous scam.

www.whatthetech.tv