TIMELY WARNING NOTICE: USF ST. PETERSBURG CAMPUS

Crime Alert Bulletin

FRAUDS AND INTERNET SCAMS

September 2nd, 2021

Just like those unwanted "Extended Vehicle Warranty" calls, frauds and internet scams are annoying and have no end in sight. Remember, the best advice is do not click on the hyperlinks and if the offering seems too good to be true, well it most likely is, so trust your instincts.

The most recent internet scam looks like this one and demands a bitcoin ransom "or else".

> Hello!
> Have you recently noticed that I have e-mailed you from your account?
> Yes, this simply means that I have total access to your device.
>
> For the last couple of months, I have been watching you.
> Still wondering how is that possible? Well, you have been infected with malware…..

Other popular scams offer lucrative and flexible job opportunities, on-line shopping deals, scholarship offerings and even social media blackmailing.

What You Can Do to Avoid a Scam

Block unwanted calls and text messages. Take steps to block unwanted calls and to filter unwanted text messages.

Don't give your personal or financial information in response to a request that you didn't expect. Legitimate organizations won't call, email, or text to ask for your personal information, like your Social Security, bank account, or credit card numbers.

If you get an email or text message from a company you do business with and you think it's real, it's still best not to click on any hyperlinks. Instead, contact them using a website you know is trustworthy.

Resist the pressure to act immediately. Legitimate businesses will give you time to make a decision. Anyone who pressures you to pay or give them your personal information is a scammer.

Know how scammers tell you to pay. Never pay someone who insists you pay with a gift card or by using a money transfer service. And never deposit a check and send money back to someone.

Stop and talk to someone you trust. Before you do anything else.

For additional information or to report a scam or fraud to the Federal Trade Commission contact https://www.ftc.gov/faq/consumer-protection/submit-consumer-complaint-ftc.

You may also access additional information and protections at this USF Information Technology webpage at https://www.usf.edu/it/documentation/phishing.aspx.

If you need any additional information or assistance, please contact the University Police at 727-873-4444 or **usfsp-police@usf.edu**.