

CHIEF'S BRIEFING



Preventing Scams

WHEN IN DOUBT,
CHECK IT OUT



Data Privacy Day occurs every January to remind individuals of the importance of online safety in an increasingly digital world. Primary issues we see at the Northville Township Police Department are stolen identities, threats involving payments requests and extortion. Given how difficult it is to identify and prosecute scammers, we're emphasizing prevention and this important rule of thumb:

When in Doubt, Check it Out.

We typically are contacted for the following types of scams:

- **Scammers identify themselves as representing an organization you know.**
 - Scammers pretend to be from the government, like the FTC, Social Security Administration, IRS or Medicare. Or they say they are from a business you know, like a utility company or cable provider. They use technology to change the phone number that appears on your caller ID.
- **Scammers tell you there's a problem, or they have money or a great investment opportunity for you.**
 - A common approach is you're in trouble with the government or you owe money. Or someone in your family had an emergency. Or there's a virus on your computer.
 - Some scammers say there's a problem with one of your accounts and you need to verify some information.
 - Others will lie and say you won money but have to pay a fee to get it.

- **Scammers will say you need to act immediately.**

- Scammers pressure you to act before you have time to think or check out their story.
- They might threaten to arrest you, sue you, take away your driver's or business license or deport you. They might say your computer is about to be corrupted.

- **Scammers ask you to pay in a specific way.**

- They often insist that you can only pay by using cryptocurrency, wiring money through a company like MoneyGram or Western Union, using a payment app, or putting money on a gift card and give them the numbers on the back of the card.
- Some will send you a fake check to deposit and send them money.

Defensive measures are helpful to avoid becoming a victim.

- Block unwanted calls and text messages.
- Don't give your personal or financial information in response to a request that you didn't expect. Honest organizations won't call, email or text to ask for your personal information, like your Social Security, bank account or credit card numbers.
- Do not click on any links. Instead, contact them using a website you know is trustworthy. Or look up their phone number. Don't call a number they gave you or the number from your caller ID.

- Resist the pressure to act immediately. Honest businesses will give you time to make a decision. Anyone who pressures you to pay or give them your personal information is a scammer.
- Stop and talk to someone you trust. Tell someone – a friend, a family member, a neighbor or your local law enforcement agency – what happened. Talking about it could help you realize it's a scam.

People often call us after they've been scammed, but these cases are difficult if not impossible to prosecute. The best defense is a good offense:

WHEN IN DOUBT, CHECK IT OUT.



Before you trust or click, CHECK PLEASE!

Use our checklist of 7 tips to learn how to avoid getting scammed.

- 01 BEWARE OF STRANGE CALLS**

Cold calls are not online scams but they are one of the most common scams in Singapore. The scammer calls to get your personal information or money. They may be intimidating or friendly, and may even know details about you through your social media. Hang up immediately and check with the organisation directly to find out if the call came from them.
- 02 KEEP YOUR PERSONAL DETAILS SAFE**

Be careful of the personal information you share online. It may be difficult to manage how it is used when it becomes publicly available.
- 03 CHECK SUSPICIOUS RECEIPTS**

If you receive an invoice for a product or service that you haven't purchased, either through post or email, check with the supplier directly. These fake receipt scams often direct you to verify your purchase through scam sites requiring your account details.

- 04 BE ALERT IF SOMEONE ASKS YOU FOR MONEY**

Be cautious trusting someone that you have not met in person, and offer emotional instead of financial support.
- 05 STAY DRESSED**

If you are persuaded or blackmailed into sending explicit photos or videos of yourself, the scammer may threaten to share them unless you pay a ransom. Be careful accepting friend requests from strangers, and stop all contact if the conversation becomes uncomfortable.
- 06 KNOW WHAT YOU SIGN UP FOR**

Some companies may ask for your card details for a cheaper or free trial of their service, then automatically charge a subscription fee. Check reviews of companies, and read the terms and conditions before signing up. Review your bank statements regularly so that you are aware of any changes in subscription charges.
- 07 CULTIVATE GOOD ONLINE HABITS**

Before giving out personal information, verify the source. Make it a point to set strong passwords and change them regularly.