SHOP SMART AND AVOID The Holidays SCAMS

SCAMS TACTICS

Phone Scams

Deceptive tactic through phone calls where scammers commonly make false promises in order to obtain sensitive information or financial gain.

SMS Scams

Known as SMISHING. This scam tactic uses deceptive text messages with the intent to gather sensitive data or money from you.

Fake Retailers

Cloned malicious sites of well-known websites where popular fake products are listed to grasp your attention. The motive is to distribute ransomware, trojans, and harvest your credentials.

Charity Scams

Fraudulent schemes that prey on your generosity by seeking donations to charities. The common ones include topics such as natural disasters, politics, veterans, and war (Ukraine).

ADITIONAL RESOURCES
Internet Crime Complaint Center https://www.ic3.gov/
https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety
* https://www.donotcall.gov/
**https://www.capitalone.com/digital/eno/virtual-card-numbers/
** https://privacy.com/virtual-card

WARNING SIGNS

PHONE SCAMS

* A claim that you have been specially selected
* Use of high-pressure sales tactics and "limited-time" offers
* Request that you "confirm your personal information"
* Request payment by means other than credit card –including cash, gift card, wire transfer or private courier
* Use of threats if you do not comply –even the threat of arrest
* The call starts with a prerecorded message, nobody on the other end –called a "robocall"
* Claims you have a virus on your computer or requests to log in to your computer
* Claims to be a friend or relative in need of money –but they do not give you any time to think or contact others

SMS SCAMS

* Prize or money awards
* Delivery notifications to track packages
* Gift cards scams
* Billing/invoice statements

Abstain from replying by text "STOP" or "NO." This action let scammers know that your phone number is active and could be sold to other bad actors. Instead, delete, block, add your phone number to Do Not Call list*, or report it to your carrier

FAKE RETAILERS

* Sites that request your credentials, poor design, no contact information
* URL has grammar, spelling, typo errors or are not secured
* Prices of products are extremely low
* Lack of safe payment methods or are untraceable
* Look for the HTTPS

CHARITY SCAMS

* Pressure to give right now
* A thank-you for a donation you did not make
* A request for by gift cards, money wire transfer, or cash

BE SMART AND STAY SAFE

01 Verify the authenticity of the retailer or sender before taking any action.

02 Pay with your credit card or virtual card rather than your debit card**

03 Use secure Wi-Fi: avoid coffee shops and free wi-fi to shop online. If you are using public Wi-Fi, use VPN or your own phone hotspot.

04 Always use traceable payments in order to have a chance of recovery if an online payment transaction goes wrong.

05 Strengthen your accounts: use unique-strong passwords for all accounts, and protect your accounts with multifactor authentication and/or One Time Password when possible.

06 Monitor your bank statements, and use a wallet service (eg. PayPal, Google wallet, or Apple wallet).

07 Never click a link or call back a number from an unexpected delivery notice. Contact the company directly using a verified number or website.

08 Be suspicious of any deals such as pricing, availability or delivery time that seem too good to be true.

09 Protect your devices when shopping online: Keep your devices up to date, install anti-malware.

10 Refrain from giving personal and financial information to anyone (Social Security number, date of birth or bank account number).

NORTH Dakota Be Legendary. | Information Technology