elements® of money

Published for the teen members of Merck Sharp & Dohme Federal Credit Union

WINTER 2024

SAFEGUARD THE DIGITAL "YOU"

Scammers work day and night, tricking unsuspecting teens into giving up money, personal information, or both. Social media platforms, online advertising, and email provide many opportunities to lay their traps. Build your defense against scams by learning what to expect so you're not a scammer's next victim.

BE ON GUARD AGAINST THESE COMMON SCAMS TARGETING TEENS:

ONLINE SHOPPING SCAMS

These often start as ads on social media or within web pages. The ad directs you to a website to purchase a product. After checkout, you wait and wait for a product that never arrives, or when it does, it's nothing like the ad. When you try to contact the "company" to get a refund, the phone number doesn't work, your email bounces back, and the website is no longer active. Your money is gone, and so is the scammer.

SOCIAL MEDIA SCAMS

Scammers create fake social media accounts to connect to you. They create a relationship through messages to build your trust and then tell a story about why you should send them money. It could be anything from "I need emergency surgery" to "my car broke down." They may ask for the money through a wire transfer, gift card, or through a money transfer app, all of which make it challenging to get your money back.

GIVEAWAY SCAMS

While it would be nice if you were "today's lucky $1,000 winner," the truth is, clicking on a post, ad, email, or text like this will cost you. These scams promise you a prize (like money or free stuff) that you only get after you pay. They may call it an "administrative fee," "taxes," or something else, but whatever they call it, it's a scam. After you pay, they have your money and personal information, and you don't get your prize.

ONLINE GAMING SCAMS

When playing an online game, you may receive a message from another player promising in-game items for free or cheap. The scammer may tell you to click on a link, which doesn't get you the promised in-game items; instead, spyware is downloaded. The spyware secretly tracks you online and records information. The scammer now has access to anything from passwords to financial information.

JOB SCAMS

These scams come in the form of job postings. You may come across them on a job search site or as an email in your inbox. They make outrageous claims like "make $500 for 10 minutes of work" and will say just about anything to get you to click on links that infect your device with malware. They often ask you to reply to an email address with your personal information or pay a "registration fee." Once you send your personal or financial information, they've got what they want.

HOW TO PROTECT YOURSELF

- **Check Them Out –** Look at a company's reviews in a search engine before buying a product. Search the company's name and "scam" to discover the truth.
- **Be Skeptical –** Not everyone on the internet is who they say they are. Do reverse image searches of profile pictures. If the details don't match up, they're a scammer.
- **Recognize the Red Flags –** Identifying signs of job scams are spelling mistakes, strange bold and uppercase letters, and a vague explanation of what the job is.
- **Less is More –** Limit who can see your social media posts and profile information.
- **Share with Care –** Never share photos or information with a person online that you don't know in real life.
- **Slow Your Scroll –** Scammers make things look very enticing to get you to click - don't fall for it! Pause your scrolling to think about if something seems too good to be true. Avoid finding out the hard way that it was.

Enter the Elements College Scholarship Challenge

A social media scholarship challenge for teens

FEATURING A $1,000 PRIZE

The Challenge is open to high school juniors and seniors around the U.S. who belong to the Elements of Money program. Paying for college is challenging, so we want to help you out! Check out elementsofmoney.com for rules and details. The challenge runs from January 24 through March 27, 2024.

SCAMTIONARY

A DICTIONARY FOR SCAM TERMS

JUICE JACKING
When a scammer loads malware onto public USB charging stations

MALWARE
"Malicious software" used to commit cybercrime

PHARMING
Redirecting users from legitimate sites to fake ones

PHISHING
A scam that aims to trick people into sharing personal or financial information

SHIMMER
A device used by scammers to steal information from a credit card's chip

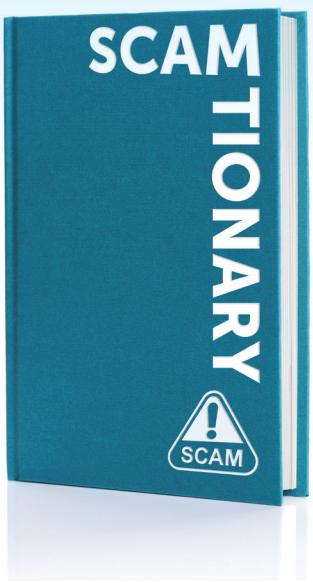
SKIMMER
A device used by scammers to steal information from a credit card swipe

SMISHING
Phishing via text message

SPOOFING
When a scammer disguises a communication to make it seem like it is coming from a trusted source

SPYWARE
A type of malware scammers use to gather data from electronic devices

VISHING
Phishing via phone; when a scammer makes deceptive phone calls



WELCOME TO ELEMENTS OF MONEY!

MERCK SHARP & DOHME
FEDERAL CREDIT UNION

(215) 996-3700
www.msdfcu.org
www.elementsofmoney.com/msdfcu

NCUA

surcharge free ATMs:

Allpoint

CU$