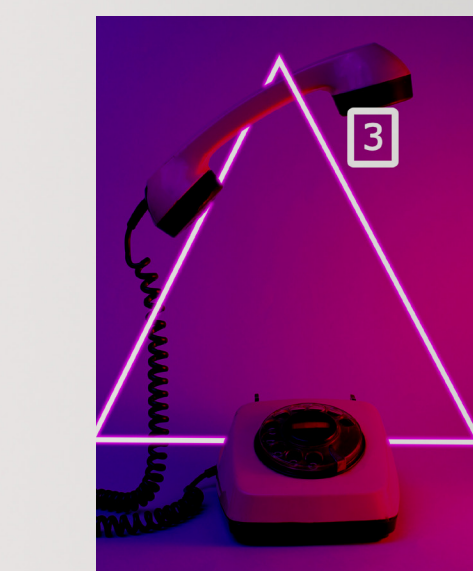




Get the look

- You know what it takes to be rad. Being rad means looking carefully at each hyperlink before you click it to make sure it won't install malware on your computer. This blazer with shoulderpads and teal shades combo lets everyone know that you **THINK BEFORE YOU CLICK**.
- Want a look that, like, screams **ENABLE MULTI-FACTOR AUTHENTICATION**? Look no further than this gnarly plastic jacket paired with neon shutter shades. Everyone will know that you don't rely on just a single password to protect your online information.



Get the gear

- You know that you should **UPDATE YOUR SOFTWARE**, but how can you be sure that your friends know you know, you know? Well for sure, this phone of the future makes it clear to all that you don't just update software as soon as you get a notification to, you have automatic updates turned on so your software is always as safe and secure as possible.
- Want to tape the latest tubular music videos by your favorite new wave artists, like the new band **USE STRONG PASSWORDS** from Iceland? This awesome TV/VCR combo lets you easily tape their latest videos like "I Use Long, Unique, Randomly Generated Passwords" and classic videos like "A Password Manager Will Secure and Encrypt Your Passwords For You."

TOTALLY OUTRAGEOUS CYBER Catalog Order Form

Use this form to order by mail...

Please include check, money order, or rolls of pennies in envelope with completed form.

Sorry, no C.O.D.'s allowed.

Will not ship to Hill Valley, CA

Totally Outrageous Cyber is, like, not responsible for, like, damages caused by, like, any purchases.

Name of Item	Catalog Number	Quantity	Monogram Initials	Price
Total:				

THANK YOU!

REMEMBER: No Refunds, No Returns! And also...

THINK BEFORE YOU CLICK: RECOGNIZE PHISHING

It's pretty bogus to steal info, but malicious actors use phishing emails and try to do it all the time, including at IHS. They're just wannabes and need you to ignore the signs that can indicate they're total fakes. If the message makes you want to take action, chill out and make sure it's the right sender. Also look for misspellings, bad punctuation, weird spacing, or requests that seem out of the norm or otherwise not legit.

UPDATE YOUR SOFTWARE

If you want stellar software security, keep it updated! Updates also improve performance, ensuring a tubular experience and easier working conditions. Keeping mobile devices updated help to protect the information on them from breaches, hacks, and even identity theft. Bad guys know about vulnerabilities and can look for devices that aren't up-to-date.

ENABLE MULTI-FACTOR AUTHENTICATION

We kid you not, using only a PIV card or user name to prove, or authenticate, your identity is not enough. The most excellent way to protect accounts is through multi-factor authentication. Your PIV or user name only prove who you claim to be. Add your PIN or password to that, and you have a schweet security solution! Anyone needing your password or PIN is a bad guy. IT Support will never ask for that information.

STRONG PASSWORDS

For mega account security, use a password that's hard for others to guess, but easy for you to remember. Our security has to work 100% of the time, but the totally uncool bad guys only have to be right once. A long password that you can remember is stronger than a complex one that you need to write down or store on your machine. There's nothing gnarly about password compromise, so make yours hard to crack!

CUSTOMER SERVICE

For any questions, please contact Cybersecurity@ihs.gov.