

REMEMBER LAST NIGHT? YOUR SOCIAL NETWORK DOES, IT LOVES TO SHARE!

IT'S GOT PICTURES!

Questions?

Contact the OIT Help Desk

Phone: 202-885-2554

E-mail: helpdesk@american.edu

IM: AskAmericanUHelp



UP YOUR PRIVACY SETTINGS, SPARE YOUR SOCIAL LIFE.



Brought to you by the Office of Information Technology
2011 Information Security Awareness Contest Poster Winner
www.facebook.com/secvideocontest

CYBERCRIME:

A WOLF IN SHEEP'S CLOTHING



Questions?

Contact the OIT Help Desk

Phone: 202-885-2554

E-mail: helpdesk@american.edu

IM: AskAmericanUHelp

Use strong passwords and ALWAYS update your computer.
DON'T BE FOOLED.
The bad guys are getting smarter.

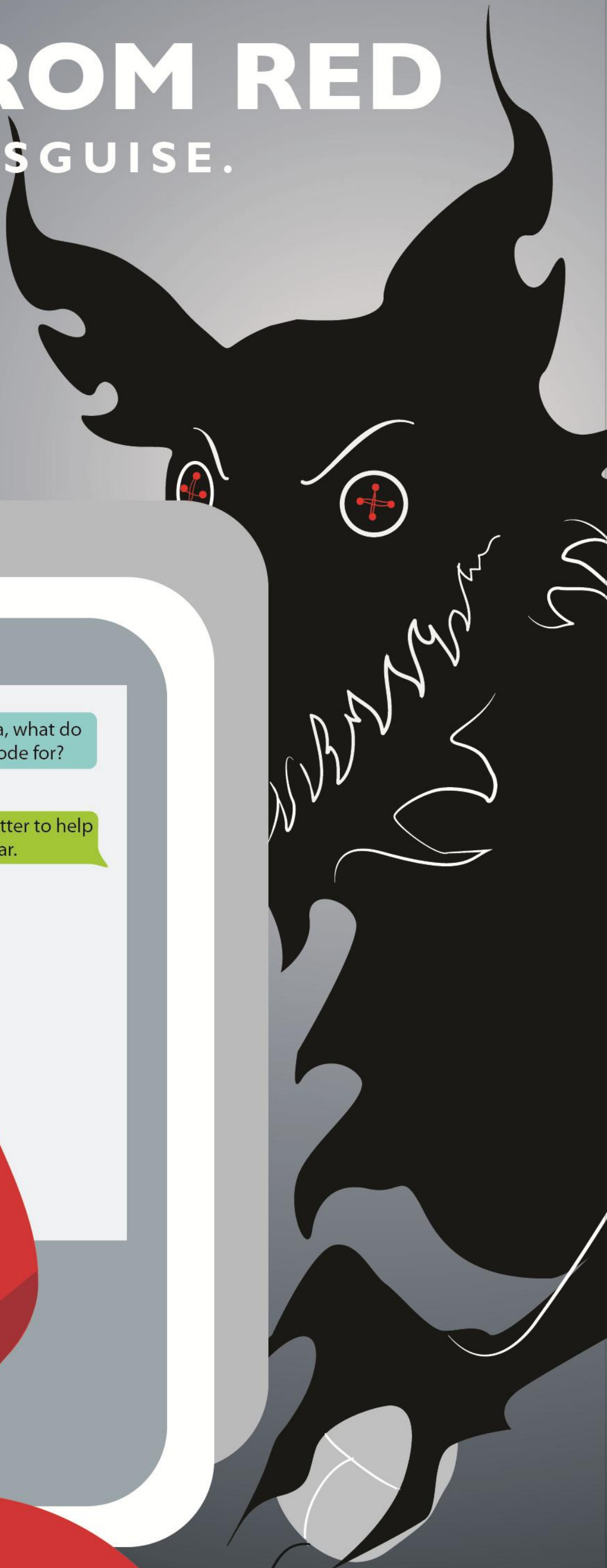


Brought to you by the Office of Information Technology

2011 Information Security Awareness Contest Poster Winner, www.facebook.com/secvideocontest

TAKE IT FROM RED

IT'S A WOLF IN DISGUISE.



RED: Why Grandma, what do you need my pin code for?

G'Ma: All the better to help you with my dear.

Questions?

Contact the OIT Help Desk

Phone: 202-885-2554

E-mail: helpdesk@american.edu

IM: AskAmericanUHelp

NEVER GIVE OUT PERSONAL INFORMATION OR PASSWORDS.

Banks, social media pages, online communities and web stores will never ask for your passwords or private information through e-mail.



Brought to you by the Office of Information Technology
2011 Information Security Awareness Contest Poster Winner
www.facebook.com/secvideocontest



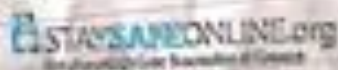
WE HAVE
YOUR
IDENTITY



Questions?
Contact the OIT Help Desk
Phone: 202-885-2554
E-mail: helpdesk@american.edu
IM: AskAmericanUHelp

Identity Theft
is a click away.
Protect yourself.

visit:
www.cyberwatchcenter.org
www.staysafeonline.org

 STAYS SAFE ONLINE.ORG
An American University Foundation of America



Brought to you by the Office of Information Technology
2011 Information Security Awareness Contest Poster Winner
www.facebook.com/secvideocontest

Questions?

Contact the OIT Help Desk

Phone: 202-885-2554

E-mail: helpdesk@american.edu

IM: AskAmericanUHelp



Lures belong in your
tackle box,
NOT your inbox.



Brought to you by the Office of Information Technology
2011 Information Security Awareness Contest Poster Winner
www.facebook.com/secvideocontest

DON'T LET A **PHISHING SCAM** REEL YOU IN

In a phishing scam, a criminal sends you an email message that appears to come from a legitimate source, like your bank or some other reputable company. The message, which may look authentic, instructs you to follow an enclosed web link—usually to “confirm your account” or “verify your information immediately.” But the link actually sends you on to a counterfeit website that looks like the real one.

Delete suspicious messages immediately, and NEVER respond to email requests for personal information.



Questions?

Contact the OIT Help Desk

Phone: 202-885-2554

E-mail: helpdesk@american.edu

IM: AskAmericanUHelp

AWARENESS

Protect yourself.



Brought to you by the Office of Information Technology
2011 Information Security Awareness Contest Poster Winner
www.facebook.com/secvideocontest

iCondom



Just kidding.
There is no such thing as iCondom.
Learn how to protect your cell phone.

What can you do to protect your cell phone from attacks?

Follow general guidelines for protecting portable devices

Take precautions to secure your cell phone and PDA the same way you should secure your computer.

Be careful about posting your cell phone number and email address

Attackers often use software that browses web sites for email addresses and cell phone numbers. By limiting the number of people who have access to your information, you limit your risk of becoming a victim.

Do not follow links sent in email or text messages

Be suspicious of URLs sent in unsolicited email or text messages. While the links may appear to be legitimate, they may actually direct you to a malicious web site.

Be cautious in choosing downloadable software

There are many sites that offer games and other software you can download onto your cell phone or PDA. This software could include malicious code. Avoid downloading files from sites that you do not trust, and check sites for website certificates.

Evaluate your security settings

Make sure you take advantage of the security features offered on your device. Disable Bluetooth when you are not using it to avoid unauthorized access. Establish a personalized access code- the standard code is "0000"- and require code entry for all Bluetooth transfers, and connections.

Questions?

Contact the OIT Help Desk

Phone: 202-885-2554

E-mail: helpdesk@american.edu

IM: AskAmericanUHelp



Brought to you by the Office of Information Technology
2011 Information Security Awareness Contest Poster Winner
www.facebook.com/secvideocontest

Tips provided by US-CERT, a part of the DHS, c2010.