Protect yourself and your workplace - understanding how to recognize cyber threats before it’s too late.

You Are the Target
What has changed?

Why are we here, yet again????

Didn’t you say ”It’s A Whole New World” last time?
What has changed?

We are outgunned, outmanned, outnumbered, outplanned

The defendants stole more than 31 terabytes of data from universities, companies, and government agencies around the world. The cost to the universities alone reportedly amounted to approximately $3.4 billion. The information stolen from these universities was used by the Islamic Revolutionary Guard Corps (IRGC).

Notably, the website also mentions that all accounts that are purchased have a one-month warranty, so if the account is cut off during that period, the purchaser will be given a new account to use.
You Are the Target!

Stage 1: Reconnaissance
- Review the organization charts.
- Review social media.
- Your “dark web” profile
- Check the school calendar.
- Send an email.

Stage 2: Elicit a Response
- Establish confidence in the relationship.
- Identify likely victims.

Stage 3: Attack
- People don’t think clearly when they are in a hurry.
- People are nice.
Know Your Attacks - Because they know you.

**SPAM**
Annoying, but not malicious

To: Phil Romig
From: Buy It Today
Subject: Today ONLY!

Dear Friend,

Today only - free socks with the purchase of a new car!

**Virus**
They want your computer, not you.

To: Phil Romig
From: A. Student
Subject: Favor?
Dr. Romig,
Could you look over this paper before I submit it?

**Harvesting**
Want your our sensitive information

To: Phil Romig
From: CCIT
Subject: Passwords
Phil Romig,
Important! Passwords must be changed today
http://mine.edu/pw

**Fraud/Theft.**
They want our money.

To: Phil Romig
From: Tom Garza
Subject: Fines
Phil,
Your parking fines are piling up again. Will you call me so we can and get them paid?
Tom (303) 237-3866
To: Phil Romig
From: Buy It Today
Subject: Today ONLY!

Dear Friend,

Today only – free socks with the purchase of a new car!
To: Phil Romig <promig3@mines.edu>
From: A. Student <astudent@mines.com>
Subject: Favor?

Dr. Romig,

Could you look over this paper before I submit it?

https://dbox.com/mypaper.pdf.exe
To: Phil Romig
From: CCIT
Subject: Passwords

Phil Romig,
Important! Passwords must be changed today
https://mine.edu/pw
To: Phil Romig
From: Mike Erickson
Subject: Passwords

Phil,

Are you around? I’m at the farm this week and the network is down again. Kirsten called and there is an emergency and I need a huge favor.
It’s Hopeless! ?

Maybe not...
The more you know about the technology, the better you will be at understanding what is, and isn’t, possible.
And none of what we can read means anything....

Inside the message can say anything at all!

It’s just a sticker!

It does have to addressed to you.

Humans can’t read the routing information, so we can’t see where it really came from.
The Old Advice is not Useless

- Spelling and Grammar
  - while much better, most attackers are still based outside the US.
- Check the To: and From: fields
  - Even though they can be faked, it doesn’t hurt.
- Does the request make sense.
  - Are you expecting a document?

Know your link

• Hover to see the hidden value.
  • http or https?

• Right-Click -> Copy Hyperlink -> Paste into Browser

• Triple check the address bar.
  • Look closely at the “domain name”, which must be between the // and the first /
Know your destination.

• While it is easy to fake the sender’s address, the response still has to go back to the sender.
Know your colleagues:

• Does the message sound like them?
• Do they use a standard signature?
• Can they spell?
• Talk and agree beforehand.
  • Pay particular attention the supervisor relationship.
Know your websites:

Shibboleth
Trailhead
Microsoft O365
The only way to be certain that an email is from someone is a cryptographic signature.

Thanks,
Phil

Philip R. Romig, Ph.D.
Chief Information Security Officer
Colorado School of Mines
(303) 273-3898

Now you know it's from me!
Final Thoughts

• Who initiated the communication
  • What do you really know about them?
  • What do they really know about you?
  • Do you really need to hurry?
• Looking at the message:
  • What are the outlook details of the sender?
  • Are messages you are sending going where you want?
• Looking at a webpage:
  • Is the domain-name correct and complete.
  • Does the URL start with https?
  • Does it look like one of the well-known Mines webpages?
Other Suggestions

DUO - stops password harvesting

When in doubt - ask.
spam@mines.edu