NOT ALL CYBER ATTACKS ARE TECHNICAL (THERE ARE SOME THAT YOU CAN PREVENT)

a guide to identifying phishing
What is Phishing?

• Phishing is the act of enticing people into voluntarily giving away credentials without realizing what is happening.

• It’s fishing for information – dangling bait hoping that somebody will bite.
Phishing Process

1. The attacker pretends to be somebody else. Common “disguises” include: another person or business, a site administrator, a bot, a person with an unusual financial situation, another website, or the owner of a hijacked account.
2. The attacker sets some bait. This could be a simple line of text in a chatroom, a link to another site, an email, or something else.
3. The victim is successfully fooled into believing that the attacker is legitimate, not a malicious pretender.
4. The victim takes the bait and enters sensitive information into a chatbox, form, or email.
5. The attacker has the victim’s information and can either impersonate the victim or sell that information.
NOW FOR TWO CLASSIC EXAMPLES
Gold Accounts

- This attack is common on user-driven sites – message boards, forums, social networking, etc.
- The attacker posts an image that claims that the victim has to purchase a “gold account” (which does not actually exist) to view the “actual” image.
  - This image is often accompanied by a comment either instructing the victim on how to “purchase a gold account” or giving information about the contents of the picture that the victim cannot see (enticing the victim to complete the transaction).
- If the victim follows the instructions or link in the image or comment, the credit card information is either given to the attacker or revealed to everybody on the site.
The Nigerian Prince
(and variations thereof)

• The attacker emails the victim claiming to be a person (a Nigerian Prince is the classic example) in an abnormal financial situation. If the victim “helps” the attacker by providing bank information, then the attacker will, according to the email, reward the victim with a significantly larger amount of money.

• If the victim falls for it, that money is gone forever. The attacker is not a deposed prince and will not pay the reward.
Another fairly common category:

WHAT HIT US
The Fake Website

• The attacker directs (in this case via hijacked email) the victim to a website that appears to be legitimate (in this case Google Drive) but is actually controlled by the attacker.

• The victim, fooled, enters sensitive information (in this case a password) into the knock-off page.

• The attacker has the information. The victim is often (as in this case) none the wiser because the attacker’s site redirects the victim to the real site.
Attack Delivery Email

• Sent by someone in the office at 7:10 PM, when the office is not open.
• References documents the victim is “expecting” without stating their subject matter.
• Just sort of suspicious-sounding in general (mostly from the wording)
The Fake Site

Website is not Google. It’s a Columbian daycare. Unencrypted connection for a login page.

Disgustingly Ugly.

Poorly-aligned elements.

Signing into Google through competitors’ services

The Real Drive Login Page

Website is actually Google.

Encrypted connection for a login page.

Clean, professional look.

Signing into Google using a Google account

Well-aligned elements.

A much more detailed page
If someone sends you to a site that doesn’t look legitimate, check:

• The page URL: is it what it appears to be?
• The connection: is it encrypted? Most browsers show a padlock icon in the address bar if it is. Don’t put important information into unencrypted pages.
• The branding: do all the logos and names make sense? Are there any that don’t? Should there be some that are missing?
• The site design: does it look professional or could some guy have thrown it together in an hour?