FIRSTSTEPS ONLINE

Security Module: Sneaky Tricks! Watch Out!

Steer clear of digital pirates sailing the online seas whose sole goal is to undermine your security and compromise your personal data and identity.

1. Beware of advertisements disguised as download buttons.

When you visit a site, you may see something to download, possibly for free, and you click what appears to be the obvious download button. Instead you are led to another form or product to buy. Worse yet, you may be led to a viral infection or malware.

If you clicked the button to the right below, would you expect to receive your requested free download?

Of course you would! However, the **“Download Now”** button on this particular site is an ad presented by a different company and transfers you to a new form to snag your personal information! The original site promises to protect your information, yet is selling your info to this advertiser! Scoundrels, they are!

And they are doing it with "your permission", so they are not violating the terms of their security agreement. How do they get your permission? Well, they didn’t. They tricked you, because buyer don’t always beware or speak Latin which is where the phrase “buyer beware” came from -- *caveat emptor.*

How to spot this trick? Hover your mouse over the button before you click it. View the full web address in your navigation bar, or in the lower left corner of your web browser, to see what the address looks like. Does it say the program or the download you expected, or does it begin with: “http://google.ads....” or some other address unrelated to the product’s website?

You can block ads like these by using an *adblocker* product from adblockplus.org. Be informed about the dangers of malware and how to spot it.

2. Don’t trust the “free” in free stuff! It’ll cost you!

Plenty of great freebies are available on the net, but some include an advertisement for the company that’s “giving” you “free” stuff.

Exhibit A, for *Actually, You’re Advertising For Us*: a company offering free or very cheap email services. The catch? Every one of *your* emails they send out contains *their* advertising.

Exhibit B, for *Bet You Didn’t Read the Fine Print*: online printing companies offering free business cards, pens, or bumper stickers with their URL

printed on each piece. To get these items without their URLs, you need to *purchase* them. No free lunch here!

If you're short of cash and you willing to offer such companies an advertising platform, then go for the free product.

Exhibit C, for *Crafty Critters, Aren't We?*; some type of attractive trial for an online service that requires you to give up your credit card information for activation. The crafty catch here? When the trial period ends, your credit card is charged. Like most buyers, you forget about the trial period and never wrote yourself a reminder about the last day of the trial, nor what to do or who to contact. You finally cancel a month after you've notice a new charge on your credit card. To cancel you have to call the company, but their customer service department is not open when you're awake because it's located in India. In their charming accent, they'll offer you an extended "free trial" and hope the same thing happens next month.

Exhibit D, for *DANGER! Your Computer Might Explode!:* a company sells virus scans or computer optimization tools and offers "free evaluations of your computer." Then they find a bevy of nasty problems and report those back to you immediately in **LARGE RED ALARMING TYPE.** To remove your life-threatening problem? You got it! You must pay!

How do you spot these scams, misleading info, or downright lies?

First, realize there's *no free lunch!* Companies don't make money unless they sell something. The purpose of a free giveaway is to let you sample their product or service, hope to win you as a customer, and maybe even drag some cash in along the way by attaching conditions to their free sample to get "value" from their giveaway.

Second, always look for the Purchase or Buy links. Know the cost structure and pricing before you buy into an offer. Only use free services of products you value enough to buy later.

If you need an auto responder, or a batch emailer, or business cards, use their free trials to *test* them... *right away*, with the deadline marked on your calendar or written in reverse type on your forehead so you can read it when you look into a mirror..

Finally, never view a free option as a solution. "Free" is seldom truly free.

3. Prevent your friends from infecting you!

Social media malware might spread through infected links your friends post on your wall. Or they might share things in their newsfeed infects everyone who opens the link. Sophisticated virus software can scan all your links and posts and flag the dangerous sites to visit.

Be sure to install a robust security product like **Norton, Kaspersky or McAfee** on your computer. These products are expensive, but compromising your information and infecting your computer can cost much more besides giving you major headaches. Free virus protection programs can be downloaded on the internet, but check them out thoroughly. They must protect your precious information and personal identity!

I make my living almost 100% online. If I lost my computer or my data for even a couple days, I'd be in big trouble. I'd search for someone to blame, and finally find the culprit *when I looked in the mirror*. It's worth the price tag to be protected.

But don't just rely on programs to save you. Here are a few things you can do to take care of yourself.

- No matter how enticing the post, do not visit sites you are unfamiliar with.
- Don't be one of the unsuspecting culprit who passes on entertaining, but dangerous posts to others!

- Beware of serial emails forwarded to you, usually containing a bad joke! Normally the joke's on you!
- Never forward serial email. I know I just said this. I'll probably say it again. Right now. Never forward serial emails. Did I say never? Never.
- Never open the attachments in any of these serial emails.
- Never download offers in a serial email. Shut off "download pictures" in your email program. Only downloaded pictures from emails you know.



Please watch a video tutorial at the end of this lesson to learn how to set up a filter in your email program to trap these emails and automatically delete them. Filter on the phrase "**Fwd or FW"** and send these emails to a subfolder or to the trash.

SPAM: It's not just "spiced ham" in a can from Hormel foods.

On the internet, **SPAM** means *unsolicited commercial emails* or **UCE**. And it's not merely annoying. It's dangerous. It's the main distributor of potentially destructive viruses – designed to destroy your computer and its contents.

An official SPAM definition from the *Oxford Dictionary*: "Irrelevant or unsolicited messages sent over the internet, typically to a large number of users, for the purposes of advertising, phishing, spreading malware, etc. Unwanted or intrusive advertising on the Internet."

The massive onslaught of offensive, unethical, criminal emails is not going to stop, unless you stop them! Every day spam attempts to hijack your bank account information, sell you drugs, make you rich, and infect you with an entire host of dangerous programs. Many people fall for it daily which in turn costs us money.

With a bit of education and real solutions to the problem, you can stop spam dead in its tracks. "Mail Washer" is a free program which stops spam before it arrives in your Inbox.

Check it out by clicking HERE!

Another highly rated free spam blocker is "Spam Fighter Pro."

Check it out by clicking HERE!

4. Free iPhone or iPad scams!

Apple devices are so desirable to the public and online scams use them as bait. You might be tempted with the reward of a free device by signing up for an online newsletter, registering at a specific website, or simply "liking" a FaceBook fan page. Usually you're required to sign up for a variety of offers from movie distributors, credit card schemes, or subscription services in order to receive your device.

The only feasible way to get a free expensive device is as a gift, win it in a competition, or steal it from your children. Treat other offers as nonsense, no matter how convincing they sounds.

If you're looking for an inexpensive Apple device or other products, try a penny auctions. Here is a safe and reliable site: **PriceBenders Auctions.** In a penny auction you place a bid raising the cost of the item by one cent. To place a bid, you must first purchase a package of bids, starting at about $.30 each. Bid costs vary with each company and the volume you purchase. Bidding continues until someone wins and bid counter stops. I've won many times and I have seen an iPad mini go for as low as $3.70!!

How can a penny auction company do this? You only pay when you place a bid. They earn every time a bid is placed and get a lot more for the item than the final price.

5. Shocking Facebook video scams!

It looks harmless. What's the scam here?

A video posted or liked by a friend appears in your newsfeed, which promises some form of salacious content involving a celebrity or beautiful young woman, or perhaps unseen news footage. Several variations of this **"click-jacking**" scam exist.

By clicking the link, all your friends will be spammed with the same video. This is probably annoying to them and embarrassing to you, depending on the content of the video.

In another variation, the spammer asks you to complete a survey or fill in a form before seeing the video and earns money when the surveys are completed.

In the worst case scenario, you'll be infected by malware and spread malware to your friends... for the bogus sake of viewing a tantalizing video which does not even truly exist.

6. Fake emails that look exactly like your PayPal, Skype, or Facebook account.

These emails might be a fake bank statement, fake billing receipt, or fake Internet Service Provider receipt. *They look exactly like your account, only they are not.* They offer special rates, special sales, or maybe cry urgently, "You need to update your credit card information."

They may be emails from your credit card company with new terms for your account, "Click here to read and accept the new terms."

Watch out for these **"phishing"** emails! (Discussed again in Module 8)

Fake PayPal Phishing

You receive an email claiming to be from PayPal, which asks you to respond due to an emergency hold or cancellation of your account. You think you must respond quickly! Now! But it's fake.

Sending fake emails like this is called "phishing" because the sender is "fishing" for your personal information. ("F" is changed to "ph" and that means "Do not take the bait!") They may ask you to:

- Visit a fake or "spoof" website and enter personal information.
- Call a fake customer service number.
- Click an attachment that installs malicious software on your computer.

Even if you're totally convinced it's real, **never** reply to the email from your accounts, **never** click any links in an email from your accounts, and **never** download any attachments from your accounts.

Did I say never again? Sorry, what I meant to say is... **NEVER!!**

I have one email account and pay an annual fee – a very secure email account. Recently I received an email that claimed my credit card didn't process correctly, and I may need to update the card. Links like this were in the email:

- Log in to your account here.
- Read updates about your account.
- Update your card information now.

Did I click any of those links? No way! Didn't I say just write **NEVER?**

I opened my browser, went directly to the account page (in a different window) and checked my account charges and balance. What did I find? No charges. My balance – zero. My credit card info – correct and up to date.

What should you do in this situation?

If you receive an email like this, or click a link seems to be a phishing attempt, or open an attachment from a suspicious email, report the email as soon as possible so your service provider can help protect you and other members. Most email services have a website or address where you can forward any phishing or suspicious emails. Paypal's is spoof@paypal.com. Once you've reported the scam email, delete it forever. To learn more about how to avoid PayPal phishing, read their Identity Protection Guide.

Skype Scammers

Fraudulent emails might ask you to provide your Skype password, payment details, or sensitive personal information. They might inform you of the need to upgrade or reinstall Skype, or your order is being delivered, or has been refused. Here are the subject lines from recent fraudulent emails:

- New Skype Has Been Released
- Download New Version Of Skype! More Free Talks
- New Version Of Skype Has Been Released! Upgrade Available Now
- Your Skype Account Has Been Limited!
- New Releases: Download New Skype 20 (??) For Your Windows And Mac

If you receive email like these, please forward these emails immediately to spoof@skype.net.

Fraudulent Facebook Emails

If an email or Facebook message looks strange, don't click any of the links. These fraudulent emails might contain these messages:

- Notifications about friend requests, messages, events, photos and videos
- False accusations that you're not following Facebook's Community Standards
- Warning you that something will happen to your account if you don't update it or take immediate action
- Claims or offers that sound too good to be true and probably are, such as, "You've won the Facebook Lottery!"

I stress again with one of my favorite words – never – even if it doesn't look strange, *never* click any links – *in that email* – which supposedly go to your account or require you to open any attachments. Please report these to FaceBook. If it's an email, forward it to phish@fb.com. If it's a Facebook message, check out this link and learn how to report messages.

Reputable businesses never require you to provide sensitive information from through an email, or through a link within an email.

Always exit the email, enter your browser, and go directly to your account site using their address that you know and can verify is correct. Check it and follow up for yourself if something is amiss.

In conclusion, use your common sense. If it sounds too good to be true, it probably is! Scams are rampant on the internet, seem to get more devious daily, and cause irreparable harm to you and your date. If you're not sure of the value exchange – your vital personal identity and details for whatever they are offering – back out! Run away! Save yourself! If it's truly a great deal, it will probably be there tomorrow.

3E's 2SUCCEED
Educate • Engage • Expand

VIDEO TUTORIAl: Creating a Filter in your GMAIL Account

Click HERE to watch

To view and read this module online, go to www.work-with-walt.com

Your purchase of this training tutorial includes free membership to the online version of **First Steps Online** which has more than 20 FREE downloadable resources.

If you have problems with login, please contact walter@firststeps.online