FIRSTSTEPS ONLINE

Security Module: Oh no! I've been Scamboozled!

As long as humans have walked on this globe, knuckle-dragging hackers and scam artists have been separating unsuspecting victims from their wealth and possessions. Your bucket list should *not* include the sinking feeling in the pit of your stomach knowing you have fallen prey to an online scam.

Has this happened to you? If so, then you are part of an elite membership called, "The Bamboozled Club." If not, be patient – a special invitation will probably be coming your way soon!

Bamboozle is defined as "to deceive or get the better of (someone) by trickery, flattery, or the like; humbug; hoodwink." (*The English Dictionary)* Bamboozle is often followed by "into", such as "They *bamboozled us into* joining the club."

I'm taking literary license and altering this word and its definition to **scamboozle,** which means:

1) to be deceived or swindled by an online scam or tricked by a cash-grabbing, internet numbskull;
2) buying a deceptive product promising lots of money in an unrealistic short period of time from a take-your-money-and-never-send-the-product charlatan;

3) purchasing a program promoted to be better than sliced bread, but delivering crumbs;
4) or a flimflam money-making scheme “limited to a very few”.

Did I leave anything out? The list could go on and on...

Another fitting word in this scenario is **digital decepticons!** These skilled language manipulators twist their sales copy and advertisements to camouflage their lack of content, imagination, and value. Not only do they use false and fraudulent words, they also omit necessary knowledge, skills, and details!

Example? “Buy my wonderful, ground-breaking product! It’s as easy as 1, 2, 3!” Deception alert! They left out numerous steps required between 1 and 2, and between 2 and 3!

Ok, I admit it! I’ve succumbed to these fast-talking, smooth-as-silk deceivers, too. I fell for a phone scammer’s pitch offering me a Promotional Giveaway –

“You get a FREE six-person fishing boat for the cost of shipping and handling! **Only $69.99!”**

Wow! Just what I needed to take my family out to the lake on a sunny Saturday afternoon! I took the bait, swallowed it whole, and received a cheap, plastic, inflatable boat worth no more than $10 – including shipping! Yes, it might hold six passengers, but only if they were skinny models right off the runway in New York! Totally embarrassed, I took a long time to live it down. Oh, yeah! I was scamboozled! (Hey! Sounds like a blues tune... uh, uh, uh, get your scamboozle down, oh yeah, yeah!)

It’s not always easy to spot a scam.

Checking with the Better Business Bureau (see below) and other watch-dogs simply is not sufficient because some scams are too new. Creativity flows very deep in Scamville, and scams often create worldwide havoc before being stopped or spotted.

When you're looking for a **work-at-home opportunity** or business opportunity, know what red flags to be aware of.

Red Flag Number 1 – Can you follow the money?

Can you figure out how the company earns money? If they're offering lifetime free services to someone and will pay you a large commission every time someone signs up, where does the money come from?

It's easy to tell yourself it can't be a scam because nobody is spending any money! You need to consider other possibilities. What information is this company collecting? What about your future customers? Can this be used against you, or them? Do you have to download anything at any point? Spyware insertion and/or affiliate commission theft could be the goal.

Red Flag Number 2 – Is the pay commensurate with your effort?

If a company offers two to three times the going rate for a job, but you have to pay for training, it's probably a scam. To cloud your judgment, they're relying on your need to earn money, and your desire to earn lots of it with little effort. Similarly, if you're earning commissions, does it look like the company can possibly make a profit? This is very similar to the first red flag above, but worth considering on its own.

Red Flag Number 3 – What kinds of promises are being made to you and to the customer? Are they even remotely possible? This could be either a bad case of exaggeration, or a sign of a scam. In either case, you don't want any part of it.

Every online opportunity isn't a scam just because it might look like one. It's possible to misjudge, but you have to decide if you'd rather avoid an opportunity that could hurt you financially and destroy your reputation, or take a chance on being scamboozled. If too many red flags are waving in your face, it's probably not worth it, but you'll have to decide for yourself.

Donald (the Duck) says, "If it looks like a duck, walks like a duck, and quacks like a duck, it's gotta be one of my kinfolk!" (I think he says this!)

So... the three relevant words here are: **Use common sense!**

This is *not* an exciting subject to discuss, I know. It's the same as telling your child, "The kitchen stove is hot! Don't touch it!" Or, "If you try to fly down the stairs like Superman, you're gonna get hurt!"

First Stepper, I hope you'll heed these warnings and never have a problem. Yet, knowingly or not, if you touch the hot stove and get burned, or put on your Superman cape on and get hurt, just remember – I'm out of Band-Aids! I apologize for sounding crass, but, that's life, and online life is no different! ☺

Most online scams fall into three categories.

Scams are all around us and found in every single area of life, but more so in areas of high risk, such as credit cards, bank accounts, and other activities involving the sending or receiving of money online. (Be sure to download the informative PDF in the 3E's to Succeed section below!)

1) The Bank/Credit Card Email Scam

An email arrives and asks you to sign up with your bank account or credit card because "your privacy is in danger" or "to receive a free gift." BEWARE! Do not sign up through the internet address provided in the email. Go to the bank or credit card site at a URL address you know is valid. If you aren't sure of the valid address, search for it on the internet.

How does this scam work?

The senders of the email know only a very few will respond, but a few suckers is all they need. When you sign up on the bogus internet address, they get your user and password, and then it's time for them to party!

2) The Missing Millionaire Scam

An email arrives in your inbox claiming the sender represent a dead or missing former ruler, high-ranking official, or businessman from Africa, the Persian Gulf, or some country you've never heard of that starts with "K", has 15 letters, and only one of them is a vowel. The email offers you a chance to earn between one to five percent of $10 to 50 Million dollars for your co-operation only! BEWARE! The only money involved will be the cash sucked from your account!

How does this scam work?

They ask for your bank details in order to transfer the cash and then use these details to transfer a small amount. Once you trust them, they ask you for more

personal and secure details because they "need" additional info to transfer the entire sum in and out of your account. What they don't tell you is they will transfer all the money out of your account – theirs and yours!

3) The Make Money Fast Scam

The most innocent of the lot is the most dangerous. A specious company advertises that if you sign up and use their “fast-cash” system which is “like having an ATM machine in your house!”

Please don’t fall for these schemes. The slimy schemers might pay you a little money, but once trust is built, they’ll fleece your bank account. Remember, quick money scams are the surest and fastest way to lose your entire wad of dough! Think this way: the lure of fast dough means you will soon have no dough!

Seven tips to spot a scam before they send you a personal invitation

1. **Something sounds too good to be true.** More than likely it is! Any offer which promises to make you rich overnight with a business that works while you sleep is a rip-off. Watch out for companies that hype major profits for minimal work, or claim “no experience is necessary.” If anyone can do it, why should you pay to learn about it?
   This practice has given multilevel marketing (MLM) a bad rap. Granted, legitimate money-making programs are out there, but so are hundreds

of over-promising, under-delivering scams. If you're considering Multi-Level-Marketing (MLM), take the time to go to www.mlmwatch.org. You can check out potential problems with most MLM groups and see how reputable they are.

2. **Companies requiring an initial investment to get you started.** *They* start and *you* don't. They get their money upfront and leave you waiting for products which never show up in your Inbox.

   Double-check the *reputation of a company* before signing up for its program. Seek references from people involved in the program, find out what strings are attached, how much money to get started, and read any "fine print." Find out how they treat their affiliates or sales people. Do they provide in-house training and support when customers have questions or problems?

   Wonderful *online training opportunities* are available which you will need to purchase up front, check them out first. If they use a reputable, certified company to process the payment, they are likely legit. Payment service providers like PayPal have measures in place for refunds and unhappy customers.

3. **Incorrect protocol or no secure encryption in the URL.** If you *do not see the letters "https"* in the company's URL in your browser, something is not right. Run away! No reputable and legitimate website that collects your personal financial data would ever omit the "https" encryption! Never ever!

4. **Misspellings and poor grammar in the copy.** Many online scams originate in countries where English is not the main language. An easy way to spot someone trying to glean your personal and private information may be right in front of you in black and white.

On the other hand, during the last three years of working online, I've seen material produced by some of the best in the business, very reputable marketers who provide an enormous amount of quality and content. Many have misspellings and an occasional grammatical error, but this may not be an indication they are scammers. Perhaps they didn't do a final spell check before going live. There's a difference, and you can use your common sense in to sort out the good from the bad.

Maybe you've found a few misspellings and grammatical faux pas in this training tutorial! Please drop me a note and tell me where so I can improve my guru-rating instead of my scam-rating! ☺

5. **A request to confirm your credit card details, bank information, or identity details.** Many scammers "clone" a financial site to make you think you're on the legitimate site of your financial institution. No reputable company, bank, or financial group will ever ask you to confirm your secure information over the phone or by email.

   This is known as **"phishing"** and you'll get more info about it below.

6. **Weird URL configurations** are dead giveaways that something's fishy and smells rotten. They could be extremely short or extra-long with strange characters in the URL. One way of knowing exactly where you'll be taken is to hover your mouse over the link or URL. Look in the bottom left side of your screen (on Google Chrome) and the true destination will show up. If you have any question about the destination, it's better to get more details before clicking.

   Use proper protection for your computer. Install a security program which builds a fortress (or firewall) around your data, personal files, and information. Free programs are available which should keep you protected from some of the major viruses and harmful attacks. As you increase your data and online working files, better protection may be required.

7. **A sense of urgency and scarcity in the message.** "You must hurry to get the last product at this special discount!" Be leery of anyone who uses hard-sell tactics or pushes you to sign up right away. When you find an intriguing program, do yourself a favor and check it out first.

What is phishing?

Fishing? No, no, no! Not talking about a high mountain lake, cool breeze blowing through your toupee, and a cooler full of cool drinks and snacks!

Phishing is an email falsely claiming to be from an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft. The email directs you to visit a website and then asks to update your personal information about credit cards, social security number, bank account numbers, and passwords.

These websites are “cloned” to look exactly like the real thing. It is relatively simple to make a website mirror the legitimate site by mimicking the HTML code or by framing parts of the pages. In the online world, you cannot believe everything you see!

People fall victim to scams designed to steal log-in information for accounts such as PayPal, eBay, and other online banking accounts. Scammers send emails to every address they can obtain, so you might receive a phishing email even when you don’t have an account with the targeted enterprise, site, or company.

The appearance of scam emails keeps getting more authentic. You may receive an email pretending to be sent from eBay with the appropriate logos and formatted the eBay way. The links within the email even seem to be directed to legitimate pages within eBay. For example, emails supposedly from eBay claim your account is about to be suspended unless you click on the provided link and update their credit card information.

Here’s a PayPal decepticon story for you.

Recently I received an email claiming to be from PayPal. It seemed to be a receipt for an eBay purchase I knew nothing about. The subject line was

"Receipt for Your Payment." The body of the email included a description of the eBay item. Below was a notice:

> *"Note: If you haven't authorized this charge, click the link below to dispute transaction and receive full refund."*

I wonder how many people receiving a similar email quickly clicked on the link provided in order to contest the charges.

OK, I already cautious with this sort of thing, so I *did not* click on anything in the email. Instead I went to PayPal on my own and logged in. Guess what? *No record* of the purchase!

I looked at the format of the email. Viewing the properties of the message, I discovered it was actually from a "takethatfanclub.com" sender and *not* Paypal. Just because the email says such-and-such.com at the top doesn't always mean that's who it's from. The "From" name in an email can easily be altered.

The formatted eBay email looked more like a received payment than an actual receipt. When I looked at my other emails titled "Receipt for Your Payment," none of them were formatted like this one.

Watch out for scams designed to trick you into submitting information (like passwords) to allow the sender to access your PayPal account.

These scams might include a message about unauthorized access attempts. The sender tells you someone has tried to hack into your account, your account is now in danger of being "frozen", but if you click the link in the email, you can enter your password to avoid the loss of your account. Folks unfortunate enough to succumb to the scam will have given their login information to strangers.

Remember: These scams are is not limited to PayPal.

Users of Storm Pay, e-gold, eBay, and others will see similar emails. Whenever you receive any suspicious messages, go to your account via *a new browser* and by typing in the URL. Never ever (and never ever again) click on a link in an email claiming to take you to your account. By doing this, your account information and your hard-earned funds will be much safer.

Think you've been scamboozled? Do this now!

If you believe you've provided sensitive financial information about yourself or any accounts through a phishing scam, do this *now*. Have you done it yet? Now have you done it? Okay, fine. Read it first and *then do it.*

- Contact your financial institution or account immediately.
- Contact the three major credit bureaus, and request that a fraud alert be placed on your credit report. Bureau phone numbers in the USA: **Equifax**, 1-800-525-6285; **Experian**, 1-888-397-3742; and **TransUnion**, 1-800-680-7289
- File a complaint with the USA Federal Trade Commission at www.ftc.gov or call 1-877-382-4357.
- Contact the Internet Crime Complaint Center at www.ifccfbi.gov if you think you've been a victim of a phishing scam.

Awareness is key in exposing scam artists around the world. When the light of truth shines on these shysters, and the proper authorities are involved, this helps everyone who is at risk and in danger of becoming a victim.

Report a fraudulent business or a potential scam here. Now.

1. If you're located in the USA, contact the attorney general in your local state.
2. The United States Postal Inspection Service (USPS) offers several pages on its website (www.usps.com/postalinspectors) about scams, including work-at-home schemes, multi-level-marketing schemes, distributorship and franchise fraud, and how to file a mail fraud complaint.
3. In the USA, file a complaint with the Better Business Bureau in the native state of the fraudulent business. The national BBB web site is www.bbb.org. You'll find a link to locate the BBB for your area, information on work-at-home scams, and how to file a complaint.
4. Report it to the United States Federal Trade Commission. They offer information on how to file a complaint, work-at-home schemes,

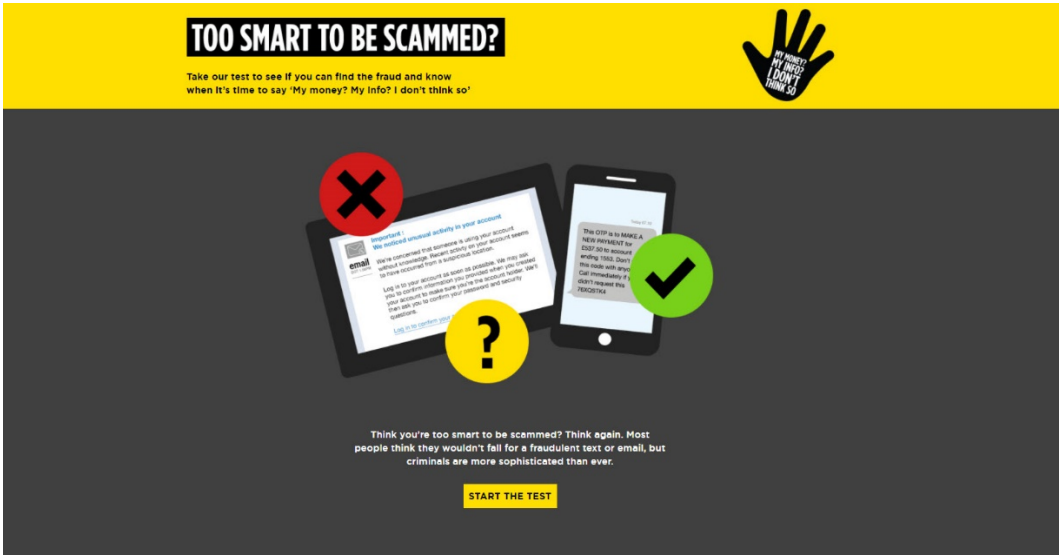
fraudulent medical billing, business opportunity schemes, the “Top 10 Dot Cons”. Call them at 1-800-876-7060 or visit www.ftc.gov/ to file a complaint.

5. List them with the Internet Fraud Complaint Center at https://www.ic3.gov/default.aspx.
6. Check the Scambusters website at www.scambusters.org – “Internet Scams, Identity Theft, and Urban Legends. Are you at risk?”
7. Take action by reporting any spam emailers to www.Spamcop.net and www.abuse.net.
8. Place a report on this website: takefive-stopfraud.org.uk/takethetest
9. For comic relief, go to www.worldwidescam.com for funny insights into the more outrageous scams in circulation.

Conclusion

Whatever you do online, always remember the internet is not a safe place. Treat it like any other business venture and keep your guard up. Play it safe by checking out companies before you commit to *anything*. Constantly protect yourself against losing money to crooks and getting **scamboozled!**

1. Download, print out, and read “10 Ways to Protect Your Web Privacy.” Click HERE to start download
2. Hey! Take this fun test to see if you can find the fraud and know when it’s time to say “My money? My info? I don’t think so!? **“Too Smart to Be Scammed?”**



Click HERE to Take the Test and check your Scam Score!

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