# SAFETY TIPS -

## 1) E- mail ID HACKING-

Hacking is a regular occurrence worldwide over the internet. Email, social networking and other online accounts are at risk from being hacked into if care is not taken to keep secure information safe. To best to prevent your web accounts from being hacked, there are various approaches you can take to stay in control and secure.

1) **Use a secured email account.**
2) **Make your email address less easy to guess.** If you include a number with your name or an unusual word, etc., it makes it harder for someone to simply guess your name by adding your first and last names together and emailing.
3) **Guard your email password.** Do not give it to anybody else, do not store it in your email Drafts folder and do not store it where it can be accessed. Your password is valuable, so treat it as such and keep it confidential.
4) **React promptly but carefully to messages about possible attacks to your email account.** If you receive a message from your email provider that they are concerned about the email being compromised, follow it up. Read it carefully though, as if the email itself is a scam, it will have giveaway signs such as bad grammar, illegitimate/spoofed logos, a click-on link to change a password (do not click, always change a password from the account itself), etc.
5) **Consider using different email accounts for different purposes.** If you want an account where you can be less careless, such as for leaving your email address all over the internet, etc., use a separate one intended just for that and leave nothing personal or sensitive on it, ever. Keep your personal email account secure using the suggestions above but also by not giving it to many people, other than those you trust.
6) **If it's too good to be true, it's suspicious.** If you receive emails promising prizes, wins, money exchanges, eternal love, etc., then be very suspicious. Never click on a link promising such things and never reply to the email either. Delete the message without actioning it any further.

## 2) OBSENCE E-Mail-

Phishing is an online con game, and phishes are nothing more than tech-savvy con artists. In a typical phishing scam, phishes send out emails, which appear to come from a legitimate company, in an attempt to scam users into providing private information that will be used for identity theft.

Phishes use a variety of sophisticated devices to steal information—including pop-up windows, URL masks which simulate real Web addresses, and keystroke loggers that capture account names and passwords.

**To protect yourself against phishing, follow these basic guidelines:**

3Fake Profile & Email ID

**1.** Look for photos in the profile.If there is only one photo of the individual in the whole profile it makes it quite clear that the account is fake.

**2**. Look for status updates,wall posts and comments.If the user hasn't updated a status for quite a long time and hasn't been involved in any wall posting or commenting of other statuses,it means that the profile is likely to be fake.

**3.** Look at the recent activities.If it is that the user has just been adding randomers and making new friends,and that there are no pages liked or groups joined,it suggests that the user is determined in jst adding people and hence the profile is fake.

**4.** Check out the friend list.If found that maximum of the friends are of the opposite gender,it can be assumed that the profile is used either for fun or for random dating.

**5.** Check the info.If found that there is no ideal links given regarding school or education institutions or workplace and that the user is looking for dating and interested in both men and women,it shows signs of fakeness.

**6.** Check the birthdate.Birth dates like 1/1/XX…..or……31/12/XX are common between fake accounts as it is quite unique and easy to type in.

**7.** Fake profiles of girls usually have a contact no. in their info. Lets face it,girls harldy will have their contact no. in public.So watch out if the user exposes info that is unlikely for general users to unveil in public.

**8.** Look out for recent wall posts,if u see loads of people asking…'THANKS FOR THE ADD….DO I KNOW YOU'……and yet the psots remains unanswered…it is bound to be a fake one.

**9.** Look for common tarits used in facebook,like.using applications such as farmville,pet society etc….and adding siblings.If these traits are not found among the user, the profile is highly inactive or fake.This point can't single handedly prove the fakeness,however this will be a supporting clue along with other points.

**10.** If you are quite certain about the profile's fakeness,and want to be absolutely sure, try browsing google for some random profile pictues. Fake profile pictures are usually selected frm google and while browsing through it,you might as well come upon the picture the user chose for the fake account.

# 3) FAKE PROFILE/ EMAIL-ID

- **Tip 1: Use Reverse image search to Identify the person in the profile picture**

  This is definitely the most accurate and fastest way of identifying fake accounts .How does reverse image search help you identify Fake accounts ? Reverse image search actually takes an image as a input and searches for similar images existing on the internet . It is pretty much like an search engine for images .

  Using reverse image search you can easily find out the real identity of the person in any profile picture . If the account is real then you will have a hard time finding out a similar photograph of the user on the internet .

- **Tip 2: Most Fake Profiles always have a Single Image**

If the profile has less than one of his or her photo, then most probably it is an fake account. Most fake accounts tend to have a single profile picture.

- **Tip 3: Check The users Timeline**

Find out when the user has joined, most fake accounts are created just less than a week before they start sending out rampant friend requests.

- **Tip 4: Beware of Fake profiles of Girls**

Most fake profiles are created with an girls identity, which is why you should never accept friend requests from unknown females.

- **Tip 5: Check the friend list**

Check out the friend list of the user. If a Fake account has many mutual friends with you, then chances are there that the Face accounts is created by one of your friends who is trying to have some fun.

Last but not the least , For the safety of yourself and others on do report the Fake Facebook accounts and request your friends to the same .

# 4) Defamatory mail

Making of false, derogatory statement(s) in private or public about a person's business practices, character, financial status, morals, or reputation. Oral defamation is a slander whereas printed or published defamation is a libel. The plaintiff must prove that the defamation was communicated to someone other than him or her. And, if the statement is not obviously defamatory, it must be shown that it carries a defamatory meaning (see innuendo) and that reasonable people would think that it refers to the plaintiff. In case of unintentional defamation, the defendant may mitigate damages or escape liability by offering an apology. Defamation with malicious intent (see malice) invalidates the defense of fair comment and qualified privilege. Defamation that imputes a criminal offense punishable with imprisonment, is usually a sufficient ground for a court action even in the absence of a proof of special damage

How do you avoid being sued for defamation? That’s easy. Don’t ever say anything interesting. If you do want to say something that might reflect negatively on someone else, there is always a chance that they will sue you for defamation.

It doesn’t matter how careful you are. Some people will sue out of spite or revenge, or to cause you financial pain, or because they feel they have to be seen to defend their reputation.

Some will sue to try to force you to retract, even though they know you’re right. Some sue for sport. But it’s rare. Usually people don’t sue, even when they have been defamed.

Still, defamation lawsuits, when they occur, are usually expensive, technical, drawn-out, stressful affairs. You are better off avoiding them if you can. So it makes sense to minimise the risks. You can do that by writing in a way that makes it hard to sue you.

Here are my twelve golden rules for minimising the risks of getting sued for defamation.

**1. Be aware of what you're saying**

In defamation cases, you are liable not just for what you say expressly, but what ordinary people will read between the lines. You are also liable for publishing a defamatory statement made by someone else, even if you quote them accurately. You need to identify any "stings" in what you write the barbs that affect someone's reputation. What will ordinary, reasonable, fair-minded people take it to mean?

**2. Control the meaning**

The first battle in a defamation case is usually over what the words mean. Don't leave this to chance. Plaintiffs like to exploit ambiguity, claiming that the audience will understand it in a defamatory sense. You should try to eliminate ambiguity and convey your meaning precisely.

**3. Only say what you can prove**

Truth is usually the most important defence in a defamation claim. Ask yourself what evidence you could put before a court if someone challenged you, and how convincing that evidence would be.

Do you have sources? Are they credible? Do they have first-hand knowledge? Would they be willing to give evidence? If you're relying on documents, do you have someone who can authenticate them?

**4. Pick the right "tier" of meaning**

Many defamatory statements involve some sort of accusation or allegation. The courts distinguish between different "tiers" of allegation, depending on how equivocally the accusation is put. At one end is an allegation of guilt – Jack is corrupt.

Next down is the suggestion that there are reasonable grounds to believe or suspect guilt – Jack is suspected of corruption; or Is Jack corrupt? Then there is an inference that there are reasonable grounds for inquiry – Police should investigate whether Jack is corrupt. It's much easier to prove a third tier meaning like this than a first tier one. You only need evidence pointing to guilt rather than proof of it.

Rules 1 and 2 above suggest that you should pick out the tier that you know you can prove.

The safest thing to do is to use the exact language of the courts: There are reasonable grounds to suspect Jack is corrupt. That may be clunky, but it will seldom leave any ambiguity for plaintiffs to exploit.

**5. Say what you don't know**

This follows from the above rules. If you are open with your audience about what you don't know, and what you're not alleging, then it's very hard for a plaintiff to argue that readers will take more from it than that.

**6. Use the language of opinion**

There's a defence called honest opinion (it used to be fair comment) for those who are expressing genuine opinions on accurate facts that are set out or understood by the audience. So make it clear that you're expressing or republishing a view.

Say "I think", "he believes", "she reckons", "they claim". Say whose opinion it is. Use phrases that are evaluative, not factual – "I think his behaviour was disgraceful". Use rhetorical questions rather than assertions of fact. Use visuals to clue readers in to the fact that they're getting opinions, as in a letters to the editor page.

Instead of making factual allegations, use the word "seems" or "appears" (Jack seems to be corrupt), which at least opens the door for an opinion defence.

**7. Make sure the opinion is based on true facts**

Ideally, you should set those facts out, and keep them separate from the opinion. The facts don't need to justify the opinion, they just need to provide a platform for it, so that the audience can tell it's an opinion and have some idea about what it concerns.

If the facts are already in the public domain, you don't need to do more than nod toward them.

**8. Put them together**

Why not take advantage of several defences at once? Jack is a police officer, I saw him at a caf being given a package by Nick; shortly afterward, the charges against Nick were dropped and Jack bought a yacht, so I think there are reasonable grounds to suspect Jack of corruption.

**9. Take particular care with allegations of criminality and allegations about what's going on in someone's mind**

If you're accusing someone of a crime, or of (for example) lying, you need to have particularly strong evidence. It is difficult to prove someone's state of mind, so you are better off talking about the person's conduct itself (what she said was false/misleading) rather than stating baldly that she lied.

**10. Take advantage of privilege defences**

The *Defamation Act* lists a set of events that are more or less safe to report on: council meetings, press conferences, public inquiries and the like.

Even if people are slagging each other during those occasions, you are insulated from defamation if you report on them in a fair and accurate manner and in good faith. Get familiar with these rules.

You should also note that you have slightly more leeway in publishing criticisms of politicians, as long as you're engaging in genuine political discussion and acting responsibly.

**11. Act ethically**

In many ways, this is your best protection against a lawsuit. If you act ethically, you're less likely to make defamatory mistakes. If you do, the people you defame are less likely to sue you.

If they do sue, you're more likely to have a defence. Even if you don't have a defence, the judge and jury are likely to be sympathetic to you and damages are likely to be lower. How do you act ethically? Conduct obvious checks. Don't rely on biased sources. Don't say more than you know. Put your criticisms to those you are criticising before you publish, and include their responses. Be measured.

Be prepared to issue a correction and apology if you get something wrong. These steps will also position you well to argue for a defence of qualified privilege. Although this defence is in flux, it may be available to publications on matters of public interest where the publisher has acted responsibly.

You should try to position yourself to take advantage of the possibility that this defence will be available.

**12. Bear in mind who you're dealing with**

Some people are much more likely to sue than others. Politicians, for example. Business people. Celebrities. People whose reputation is important to their livelihood and have the resources to take action. Also, take extra care writing about police and journalists. And, of course, lawyers …

# 5)OBSCENE SMS/CALL

A large number of unwanted calls/texts are to randomly selected numbers where the caller continues to dial that number and annoy the recipient of that call.

Stay calm and try not to show any agitation or distress if the call is malicious or abusive.

- Log all calls by noting the date, time and duration of calls. This helps establish a pattern.
- Try to determine whether the caller is male or female, their approximate age, any accent or if there is any background noise.
- Try to think of anyone you may suspect of making the calls.
- Issue a formal warning to the Offender **"I will be laying a complaint with the Police. Do not call me again"**. Note the date and time of the warning in the log.
- If the calls are of a life threatening nature, contact the Police immediately.
- Consider having your telephone number changed to not published e.g. unavailable with directory assistance. If you have an unpublished listing be careful about giving this number out. Changing your number without making your new number not published with directory services means it is available anyone through directory services (018).

# 6) CREDIT /DEBIT CARD FRAUD

Becoming a victim of credit or debit card fraud can be a very difficult experience, and one we would never recommend you experience. While we cannot guarantee that these tips will prevent you from ever experiencing this situation, we do believe that they will help you have a higher chance of avoiding it.

- Always take the time to check ATMs and gas pumps for extra devices that may have been placed by fraudsters attempting to skim your card details. Do not use any ATM with loose parts or keypads missing the standard Braille dots - inform the bank or gas station of the potential problem and find another location to perform your transaction.
- Be vigilant when using an ATM to avoid intentional distraction by fraudsters attempting to steal your card. Fraudsters have also been known to "shoulder surf" at the ATM in an attempt to view a victim entering their PIN, so be conscious of anyone very near to you at the ATM.
- Try to avoid using standalone ATMs often found in convenience stores, hotels, bars, etc. Devices which intercept and record the ATM phone line tones can be utilized more easily in these locations than in more permanent ATM installations.
- Take the time to carefully check your credit card statement for unauthorized charges. Checking recent activity online daily or weekly is even better than waiting for your statement (but be sure to follow Safe Internet Browsing practices when doing so!).
- If your bank stores electronic copies of the checks you have written for online viewing, petition the bank to blur (or remove) the routing/account numbers on the bottom of the check. This will prevent fraudsters from obtaining the necessary information to perform an ACH (Automated Clearing House) transfer should your online banking credentials be compromised.
- Never use your debit card for online purchases. It is much more difficult and time consuming to recover lost funds from a checking/savings account than it is to contest charges with a credit card company. Designating one credit card for online purchases only is also prudent because it limits exposure and allows you to quickly identify the method of compromise.
- Explore using a credit card company that allows you to create secure virtual card numbers that are valid only for the first vendor they are used with, and which you can selectively disable without having to change your permanent credit card number.
- Avoid using computers you do not have full control over for online banking. This includes any public venue that provides a computer with Internet access.
- Be aware that if you give your debit/credit card to a restaurant employee for payment, when the employee walks away to charge the card it is relatively trivial for that employee to copy the card's magnetic stripe using a small handheld skimmer. These skimmers allow fraudsters to replicate your credit card at a later date for fraudulent transactions. This is why when you dine in the European Union, a restaurant employee often brings the mobile card processor to your table.

# 7) INTERNET BANKING

### 1. Choose an account with two factor authentication

Try to get a bank account that offers some form of two factor authentication for online banking.

These days many, but not all, banks offer a small device that can be used to generate a unique code each time you log in. This code is only valid for a very short period of time and is required in addition to your login credentials in order to gain access to your online account.

### 2. Create a strong password

If your bank requires a user-generated password in order to access online accounts make sure you choose one that is strong. The best way to achieve this is by making it long and a mix of upper and lower case letters, numbers, and special characters.

Always avoid using any common words or phrases and never create a password that contain your name, initials, or your date of birth. If your bank allows it, change your password every few months.

When setting up online banking, if your bank asks you to provide answers to some standard security questions remember that the answer you give doesn't have to be the *real* one.

So you don't have to answer "Thumper" to the name of your first pet - make it something else, as if it was a password. Use a password manager if you are concerned about how to remember everything!

### 3. Secure your computer and keep it up-to-date

Security software is essential these days, regardless of what you use your computer for.

As a minimum, make sure you have a firewall turned on and are running antivirus software. This will ensure you are protected from Trojans, keyloggers and other forms of malware that could be used to gain access to your financial data.

You'll also want to keep your operating system and other software up-to-date to ensure that there are no security holes present.

### 4. Avoid clicking through emails

No financial institution worth their salt will send you an email asking you to provide any of your login details.

If you receive an email that appears to be from your bank that asks for such details then treat it with suspicion as it may well be a phishing attempt to trick you into handing your credentials over.

Likewise, be aware of links in emails that appear to be from your bank – this is a trick often employed by the bad guys to get you onto a website that looks like your bank. When you log in to 'your account' they will steal your username and password and, ultimately, your cash.

It is always safer to access your online bank account by typing the address into your browser directly.

Also, be aware of unsolicited phone calls that purport to be from your bank. While your financial institution may require you to answer a security question, they should never ask for passwords or PINs (they may ask for certain letters or numbers from them, but never the whole thing).

If in doubt, do not be afraid to hang up and then call your bank back via a telephone number that you have independently confirmed as being valid.

### 5. Access your accounts from a secure location

It's always best practice to connect to your bank using computers and networks you know and trust.

But if you need to access your bank online from remote locations you might want to set up a VPN (Virtual Private Network) so that you can establish an encrypted connection to your home or work network and access your bank from there.

Look for a small padlock icon somewhere on your browser and check the address bar – the URL of the site you are on should begin with 'https'. Both act as confirmation that you are accessing your account over an encrypted connection.

### 6. Always log out when you are done

It is good practice to always log out of your online banking session when you have finished your business. This will lessen the chances of falling prey to session hijacking and cross-site scripting exploits.

You may also want to set up the extra precaution of private browsing on your computer or smart phone, and set your browser to clear its cache at the end of each session.

### 7. Set up account notifications (if available)

Some banks offer a facility for customers to set up text or email notifications to alert them to certain activities on their account. For example, if a withdrawal matches or exceeds a specified amount or the account balance dips below a certain point then a message will be sent.

Such alerts could give quick notice of suspicious activity on your account.

### 8. Monitor your accounts regularly

It should go without saying that monitoring the your bank statement each month is good practice as any unauthorised transactions will be sure to appear there.

But why wait a whole month to discover a discrepancy? With online banking you have access 24/7 so take advantage of that and check your account on a regular basis. Look at every transaction since you last logged in and, if you spot any anomalies, contact your bank immediately.

# 8) ONLINE LOTTERY FRAUD

**1. Any lottery or sweepstakes requiring upfront fees is a scam.** The one exception involves "skill contests" (solving puzzles, submitting recipes, etc.), where participation may legally require a small entry fee or purchase.

But know that if you do win a legitimate contest, a portion of your jackpot may immediately be withheld for federal and state taxes, and you're responsible to pay any balance when filing that year's taxes (the IRS and your home state are notified of winners).

**2. If you didn't enter a contest, you didn't win — no matter what you may be told.** If you play Powerball or a state lottery and win, it's up to you to produce the ticket as proof; lottery officials don't contact you.

**3. If congratulations come with a check — with instructions to deposit it and send a portion back — the check's a fake.** No legitimate contest issues partial-payment checks and asks for a portion back. Counterfeit checks are often used in lottery scams. Your bank may accept them and credit your account. But if you forward any funds, you'll lose them and will be on the hook for any other money drawn from that deposit.

**4. Beware of regional rip-offs, too.** Scammers sometimes set up phony state lottery websites The latest spin: county-themed cons, like one recently targeting seniors and veterans and purporting to be from San Diego County in California.

**5. The $7,000-a-week-for-life prize** in the popular Publishers Clearing House contest will be announced Nov. 26, and mailings for 2014 will follow months later. So prepare for a new season of scams claiming you've won the PCH.

**6. Duped once? You'll be targeted again, maybe right away.** If you send upfront fees for a contest, expect to be hounded for additional fees to claim that same nonexistent prize. It may be touted as a larger jackpot than originally promised. And your name will likely find its way onto scammer-shared "sucker lists" that detail names, contact info and even specific pitches that victims fall for, for use in future fake winning notifications.

**7. Clues to a sweepstakes swindle are often in the fine-print "rules."** It's a sure scam if any of the following required info is missing: start and end dates; judging date; methods of entry including judging criteria; type of proof of purchase required; description of prizes and

approximate retail values; legal disclaimers; and sponsor's name and address. Even with these included, it's wise to do an online check of the contest name before entering.

**8. If a "skill" contest seems too easy, it may be a scam.** Likely the real purpose is to collect entry fees and personal information. Legit contests only ask for your name, address, email or phone number. It's identity thieves who seek more sensitive data, such as Social Security numbers and driver's license and bank account numbers.

**9. Told you're "guaranteed" to win something? Another scam,** since that claim is usually illegal. The same applies to simulated checks or items of value in sweepstakes or skill contests that don't prominently bear the words "SPECIMEN" or "NON-NEGOTIABLE."

# 9) SIM CARD FRAUD

SIM-Swap Fraud involves a fraudster issuing a duplicate SIM card which is registered under your name. With a SIM card that shares the same number, the fraudster can stalk and save your bank related information via mobile banking transactions.Always stay alert and follow these easy to follow tips to stay safe.

Tips to prevent a SIM-Swap Fraud

- Enquire with your mobile operator if you have no network connectivity and you are not receiving any calls or SMS for unusually long periods.
- Do not neglect messages sent from your network provider that highlight a probable SIM-Swap.Remember to respond quickly to such messages.
- Never switch off your smartphone in the event of you receiving numerous unknown calls.It could be a ploy to get you to turn off your phone and prevent you from noticing a tampered network connection.Even if you are frustrated by such events, do not switch off your smartphone.
- Register for instant alerts (both SMS and Emails) that inform you of any activity regarding your bank account.
- Check your bank statements and online banking transaction history regularly so you can identify any issues or irregularities.Almost all the banks offer mobile applications to their customers which let them pay their bills,recharge their mobiles,book bus tickets etc., also let the user to have a look at the last 5 transactions, enquire the balance etc., Use such mobile banking applications to stay safe as you continue to enjoy the benefits of convenient and secure banking.

# 10) Online JOB fraud

- **You didn’t contact them, they contacted you:** They say that they “found your resume online”. They either offer you a job right away or say they want to interview you. Sometimes the scammers will try to entice you by saying that you made the cut and they are interviewing the finalists for the job.

- **You get the job right away.** After a quick phone or Instant Message interview, the 'interviewer' immediately contacts you to offer you the job.

*Tip:* Scammers troll job boards looking for victims. To reduce the chance you'll get scammed, use job sites that have privacy policies and only allow verified employers to view the listings.

**2. Vague Job Requirements and Job Description:** Scammers try to make their emails sound believable by listing 'job requirements'. Usually these requirements are so ridiculously simple that almost everyone qualifies: "Must be 18 years old", "Must be a citizen", "Must have access to the internet.' (You wouldn't be reading their email if you didn't have internet access, right?) The 'job requirements' don't mention years of education or experience. As a rule of thumb, if it's a real job, the requirements will be quite specific.

Job scam emails usually don't include clear job descriptions, either. Many of my readers say that when they ask for a job description or list of job duties, they get the brush-off. The interviewer either ignores the questions or says something like "Don't worry, we'll train you."

**3. Unprofessional Emails:** Some emails from scammers are well-written, but many aren't. Real companies hire professionals who can write well. If the email contains spelling, capitalization, punctuation or grammatical mistakes, be on your guard. Here's an example submitted by a reader:

*"The Human resources have just reviewed your resume due to the one you posted on www.allstarjobs.com.You are now scheduled for an interview with the hiring manager of the company.Her name is Mrs Ann Jernigan,you are required to setup a yahoo mail account(mail.yahoo.com) and a yahoo instant messenger"*

**5. Emails don't include contact info or are sent from a personal email account.** If the email doesn't include the company's address and phone, it's a good bet that it's a scam. And it's a good bet that it's a scam if the interviewer makes an excuse for using a personal email address by saying 'the company's servers are down", or "the company is experiencing too many problems with spam" or "the company hasn't yet set up its email system."

**6. Search results don't add up.** Before agreeing to an interview, do your research. If it's a real company, you should be able to find information about the company by doing an online search. Finding information does not guarantee that the company is legit, but if you can't find anything, you can bet it's a scam.

Some scammers pretend to represent real companies. One of our readers reported that she received a job offer from 'Proctor and Gambel', but the real company is named 'Procter & Gamble'. Another reader says that he was offered a job by someone who claimed to represent Gloprofessionals, but when he did his research, he found out it was a scam:

*"ALWAYS contact the REAL company or business and ask if this employee exist, that is how I found out this employee was a fraud."*

*Tip:* Sophisticated scammers sometimes set up nice-looking websites -- but looks can be deceiving. Try this: go to the Domain White Pages and type the company's web address into

the “domain or IP address” box and click the “go” button. The results will tell you the date when the website was created. If the website is less than a year old, be on your guard.

*Tip:* When searching for information about the company, search for both the company’s name and the email address. Also copy/paste paragraphs from the email into the search box. Scammers may change the company name but re-use the other parts of the email, and it’s possible you’ll find an identical email posted online.

**7. You’re asked to provide confidential information.** Some scammers ask for your bank account information to set up direct deposit or transfer money to your account, or ask you to open a new bank account and provide the information to them:

“*The job on offer was a "Date Entry Clerk" However, the very first item asked for by the fraudulent employer is for me to open a bank account with USAA bank, and then forward the full details of that account to Mary with the intention of adding the account the accounting department data base and to "fund the account". By full details, I mean account name, PIN code, security questions, etc. No real employer should ask for such details to send you a pay check!!!”*

Other scammers will tell you to go to a website and fill out a credit report form or provide confidential information so they can “put you on the company insurance.” Identity theft scams try to get you to provide your Social Security number and birthdate and other personal information.

*Tip:* Before entering personal information online, check to make sure the website is secure by looking at the web address bar. The address should be https:// not http://

**8. They say they will send you money or valuables, or they want to use your personal bank account to transfer funds.** Some of my readers tell me that they’ve received checks that look like real cashiers checks. They are instructed to deposit the check, keep some of the money for themselves and send the rest of the money to someone else via Western Union or MoneyGram. Then, a few days or weeks later, they get a call from the bank saying the check is fake. They have lost money they sent. Here’s an example from a reader:

*“Once you receive the check, First of all i want you to head right away to your bank, and get the check cashed. Deduct your first week pay which is $500, and Deduct extra $100 for the Money Gram sending fee and proceed to the nearest Money Gram outlet around you to make payment to my wife travel agent.”*

Some scammers ask to use your personal bank account to transfer money from one account to another account. This is called money laundering and it’s against the law. Other scams ask you to receive and forward packages from your home. These packages might contain stolen goods or illegal substances.

**9. They want you to pay for something.** Legitimate companies don’t ask for money. If you’re told that you need to purchase software or pay for services, beware.

- # 11) Internet hacking fraud definition

  - A crime in which the perpetrator develops a scheme using one or more elements of the **Internet** to deprive a person of property or any interest, estate, or right by a false representation of a matter of fact, whether by providing misleading information or by concealment of information.
  - Saftey Tips
  - **1. Choose a secure ecommerce platform.** "Put your ecommerce site on a platform that uses a sophisticated object-orientated programming language," says Shawn Hess, software development manager,
  - "We've used plenty of different open source ecommerce platforms in the past and the one we're using now is by far the most secure," Hess says. "Our administration panel is inaccessible to attackers because it's only available on our internal network and completely removed from our public facing servers. Additionally, it has a secondary authentication that authenticates users with our internal Windows network."
  - ead this whitepaper to discover best practices that drive brand affinity, repeat business and
  - **2. Use a secure connection for online checkout--and make sure you are PCI compliant.** "Use strong SSL [Secure Sockets Layer] authentication for Web and data protection," says Rick Andrews, technical director, Trust Services,
  - "It can be a leap of faith for customers to trust that your ecommerce site is safe, particularly when Web-based attacks increased 30 percent last year. So it's important to use SSL certificates "to authenticate the identity of your business and encrypt the data in transit," Andrews says. "This protects your company and your customers from getting their financial or important information stolen." Even better: "Integrate the stronger EV SSL [Extended Validation Secure Sockets Layer], URL green bar and SSL security seal so customers know that your website is safe."
  - "SSL certificates are a must for transactions," Hess agrees. "To validate our credit cards we use a payment gateway that uses live address verification services right on our checkout," he says. "This prevents fraudulent purchases by comparing the address entered online to the address they have on file with their credit card company."
  - **3. Don't store sensitive data.** "There is no reason to store thousands of records on your customers, especially credit card numbers, expiration dates and CVV2 [card verification value] codes," says Chris Pogue, director of Digital Forensics and Incident Response at Trustwave.
  - "In fact, it is strictly forbidden by the PCI Standards," Pogue says. He recommends purging old records from your database and keeping a minimal amount of data, just enough for charge-backs and refunds. "The risk of a breach outweighs the convenience for your customers at checkout," he says. "If you have nothing to steal, you won't be robbed."
  - **4. Employ an address and card verification system.** "Enable an address verification system (AVS) and require the card verification value (CVV) for credit card transactions to reduce fraudulent charges," says Colin O'Dell, lead Magento developer for Unleashed Technologies.
  - **5. Require strong passwords.** "While it is the responsibility of the retailer to keep customer information safe on the back-end, you can help customers help themselves by requiring a minimum number of characters and the use of symbols or numbers," says Sarah Grayson, senior marketing manager for the Web Security Group at McAfee. "Longer, more complex logins will make it harder for criminals to breach your site from the front-end," she says.

- **6. Set up system alerts for suspicious activity.** "Set an alert notice for multiple and suspicious transactions coming through from the same IP address," advises Deric Loh, managing director at digital agency Vault Labs. Similarly, set up system alerts for "multiple orders placed by the same person using different credit cards, phone numbers that are from markedly different areas than the billing address and orders where the recipient name is different than the card holder name."
- **7. Layer your security.** "One of the best ways to keep your business safe from cybercriminals is layering your security," says Grayson. "Start with firewalls, an essential aspect in stopping attackers before they can breach your network and gain access to your critical information." Next, she says, "add extra layers of security to the website and applications such as contact forms, login boxes and search queries." These measures "will ensure that your ecommerce environment is protected from application-level attacks like SQL (Structured Query Language) injections and cross-site scripting (XSS)."
- **8. Provide security training to employees.** Employees "need to know they should never email or text sensitive data or reveal private customer information in chat sessions as none of these communication methods is secure," says Jayne Friedland Holland, chief security officer and associate general counsel at technology firm NIC Inc..
- "Employees also need to be educated on the laws and policies that affect customer data and be trained on the actions required to keep it safe," Holland says. Finally, "use strict written protocols and policies to reinforce and encourage employees to adhere to mandated security practices."
- **9. Use tracking numbers for all orders.** "To combat chargeback fraud, have tracking numbers for every order you send out," advises Jon West, CEO, AddShoppers, a social commerce platform for retailers. "This is especially important for retailers who drop ship."
- **10. Monitor your site regularly--and make sure whoever is hosting it is, too.** "Always have a real-time analytics tool," says Punit Shah, director of Marketing at online jeweler My Trio Rings. "It's the real-world equivalent of installing security cameras in your shop. Tools like Woopra or Clicky allow you to observe how visitors are navigating and interacting with your website in real time, allowing you to detect fraudulent or suspicious behavior," he says. "With tools like these we even receive alerts on our phones when there is suspicious activity, allowing us to act quickly and prevent suspicious behavior from causing harm."
- Also, make sure whoever is hosting your ecommerce site "regularly monitors their servers for malware, viruses and other harmful software," says Ian Rogers, SEO and Web developer, Mvestor Media, an SEO and website design company. "Ask your current or potential Web host if they have a plan that includes at least daily scanning, detection and removal of malware and viruses on the website."
- **11. Perform regular PCI scans.** "Perform regular quarterly PCI scans through services like Trustwave to lessen the risk that your ecommerce platform is vulnerable to hacking attempts," advises West. "If you're using third-party downloaded software like Magento or PrestaShop, stay on top of new versions with security enhancements," he says. "A few hours of development time today can potentially save your entire business in the future."
- **12. Patch your systems.** "Patch everything immediately--literally the day they release a new version," says Kyle Adams, chief software architect for Junos WebApp Secure at Juniper Networks. "That includes the Web server itself, as well as other third-party

code like Java, Python, Perl, WordPress and Joomla, which are favorite targets for attackers."

- Popular On CIO.com

- Breached sites are constantly found running a three-year-old version of PHP or ColdFusion from 2007," says Pogue. So it's critical you install patches on all software: "Your Web apps, Xcart, OSCommerce, ZenCart and any of the others all need to be patched regularly."
- **13. Make sure you have a DDoS protection and mitigation service.** "With DDoS [Distributed Denial of Service] attacks increasing in frequency, sophistication and range of targets, ecommerce sites should turn to cloud-based DDoS protection and managed DNS services to provide transactional capacity to handle proactive mitigation and eliminate the need for significant investments in equipment, infrastructure and expertise," says Sean Leach, vice president of Technology, Verisign.
- "The cloud approach will help [ecommerce businesses] trim operational costs while hardening their defenses to thwart even the largest and most complex attacks," he argues. "In addition, a managed, cloud-based DNS hosting service can help deliver 100 percent DNS resolution, improving the availability of Internet-based systems that support online transactions and communications."
- **14. Consider a fraud management service. "Fraud does happen. And for merchants, the best resolution is to make sure you are not holding the bag when it does," says Bob Egner, vice president of Product Management at EPiServer, a .NET content management and ecommerce product company. "Most credit card companies offer fraud management and chargeback management services. This is a practical approach to take because most security experts know there is no such thing as 100 percent safe."**
- **15. Make sure you or whoever is hosting your site is backing it up--and has a disaster recovery plan. "Results from a recent study by Carbonite revealed businesses have big gaps in their data backup plans--putting them at risk for losing valuable information in the instance of power outage, hard drive failure or even a virus," says David Friend, CEO of Carbonite. So to make sure your site is properly protected, back it up regularly--or make sure your hosting service is doing so.**