Cards by Category
Cards Matched for You
Credit Card Deals
Balance Transfers
0% APR
Low Interest
Cards for Business
Rewards
- Cash Back
- Gas
- Travel & Airline

Instant Approval
Cards for Students
Prepaid
Secured

Cards by Credit
Excellent Credit
Good Credit
Fair Credit
Bad Credit
Limited or No Credit History

Cards by Issuer
American Express
Bank of America®
Barclaycard
Capital One®
Chase®
Citi®
MasterCard®
U.S. Bank
USAA Bank
Visa®
All Credit Card Companies

Credit Card News
News & Advice
Charge-it Blog

Tools
CARDMATCH™
Glossary

10 ways to protect your cards when traveling

By Matt Alderton
March 4, 2016

Email Tweet Like 9 G+1 1

Whether traveling for business or pleasure, keeping an eye on your cards and personal data is something you need to be vigilant about from airports and hotels to local restaurants.

In January, Hyatt Hotels Corp. said that 250 Hyatt hotels in 50 countries were affected by data breaches between August and December 2015. Cybercriminals used malware to steal payment card data — including cardholder names, card numbers and expiration dates. Similar breaches have occurred at hotels operated by Hilton, Starwood, Mandarin Oriental, White Lodging and Trump Hotels.

Hotels are just one worry.

"Travel exposes more vulnerabilities because you're typically doing more things out of the normal that expose your personal identifying information," says Paige Hanson, chief of identity education at LifeLock.

With a business trip, for example, you use your credit card or app to get to the airport, check in with your driver's license or passport, have a ticket printed with your personal identifying information, go through security and show your personal identifying information to another person.

"Once through security you may grab a bite to eat and use a credit card," Hanson says. On your flight, you might decide to get some work done and use the plane's Wi-Fi. "When you're online you also check your personal email, social media and credit card statement," Hanson says.

Indeed, employees who frequently travel for work are 66 percent more likely to have been a victim of identity theft compared to individuals who do not travel for work, and international travelers are almost three times more likely than the average person to have been a victim, according to LifeLock research.

"Now imagine it's a family trip and you're exposing all of their information, too," Hanson says. "Being more vigilant could save you a lot of time, hassle and frustration when you're back from your travels."

> ***"As time-consuming as it can feel to make sure that all of your information is protected online and off, it's not as difficult as resolving your accounts and reclaiming your identity once it's been stolen."***
> *— Michelle Schofield, Jumio's senior director of global marketing*

Whether traveling to Paris, Texas, or Paris, France, here are 10 ways to be more vigilant when you're away from home:

1. Keep track of your travel documents.
Although it's trash to you, your boarding pass might be treasure to a thief, says Michelle Schofield, senior director of global marketing at ID authentication company Jumio. "These passes don't just have your flight number and boarding time; the QR codes can give criminals access to all the information listed in your airline account," she says.

"This means hackers may have access to your personal information — including home address, birthday and credit card information — as well as access to all future flights tied to your frequent flier account.

"These details also may make it easier for a cybercriminal to reset the PIN number used as protection on your frequent flier account, or use that PIN to hack into other accounts."

To keep your boarding pass out of criminals' hands, shred paper travel documents when you're done using them and use a mobile boarding pass whenever possible.

2. Pre-pay your way.
Prepaid travel cards offer added security — you're using debit and credit cards less — and may help you keep from overspending while on vacation. Preload the card to pay for your travel expenses and you can use it to make reservations, to get cash at ATMs, to pay for merchandise and as a hedge against currency risk.

John C. Lightcap, founder of the website Travel-Safer.com and author of "The Travel Safety Handbook," likes the new Travelex multi-currency Cash Passport prepaid debit card. "Keep in mind it is only available in euros, British pounds, Canadian and Australian dollars, yen and pesos," he says.

3. Choose credit over debit.
"Try to use a credit card over a debit card. If your card is breached, it may be easier to dispute the charges with your financial institution," says Hanson.

Credit cards offer more consumer protections for fraudulent purchases than debit cards do, but debit card users do have recourse.

With credit cards, the federal Fair Credit Billing Act guarantees that a cardholder is only on the hook for the first $50 in fraudulent charges. However, Visa, MasterCard, American Express and Discover offer zero liability, meaning you owe nothing as long as you report the fraud within 60 days of spotting it.

With debit card fraud, a card user's liability also is limited to $50, but only if you report the fraud within two business days after you find out about it. If you wait longer, but notify your bank within 60 days, your liability is capped at $500. Delay even longer and you might be out the full amount.

> ***"Try to use a credit card over a debit card. If your card is breached, it may be easier to dispute the charges with your financial institution."***
> *— Paige Hanson, chief of identity education at LifeLock*

4. Make sure you've got chip cards before your trip.
Hanson also recommends carrying only chip-embedded cards, if possible. Chip cards are more secure than the old magnetic stripe cards. The chip in your card sends encrypted information to the terminal, including a digital key that can only be used once. The information from the chip allows your card to be authenticated.

While chip-and-PIN cards are more secure (and more commonly used overseas) than chip-and-signature cards (now common across the United States), either chip card variety is more secure than the old magnetic stripe cards, security experts say.

5. Keep your vacation to yourself.
Although you probably want to brag about your travel plans on social media or post the requisite vacation selfie, you might want to hold off until you return, says Schofield.

"In addition to a heightened risk of a potential home robbery, if a criminal knows what area you're traveling to, they can rack up purchases in that location while your credit card company won't flag them as suspicious," she says. "Save the vacation photos and updates until after you're back home."

6. Avoid public Wi-Fi.
If you're going to be connecting to the Internet at the airport, on your flight or at your hotel, use a virtual private network (VPN) service, which allows you to use a public network to access a private Internet connection.

"VPNs protect your data by re-routing it through their private servers, which take the data and encrypt it before it gets to its intended destination," says Lightcap. "My favorite analogy is to think of internet data as a straw in a movie theater sized soda. VPNs add a straw within that straw for your data so it is shielded from the rest of the people collectively using the main data stream.

"There are plenty of free options; however, I prefer the extra features that a paid account provides. I use Private Tunnel."

7. Keep your eye on your cards at all times
Never let your cards out of your sight — even at a restaurant, advises frequent traveler Suzanne Garber, CEO of Gauze, a global hospital database created for use by international travelers.

"Do not leave your credit card alone with anyone," she says. "This means waiters, gas station attendants or anyone in between.

"In fact, in many countries, waiters routinely bring the consumer the credit card machine in order to swipe the card in front of the consumer. The U.S. is one of the last countries to practice the outdated process of removing a card from a consumer's sight for payment," she says. "If the machine can't be brought to you, go to the card-reading machine."

> ***"Do not leave your credit card alone with anyone. This means waiters, gas station attendants or anyone in between."***
> *— Suzanne Garber, CEO of Gauze*

8. Be wary of ATMs.
When using an ATM, look for signs of card skimmers, such as if something is loose, crooked, colored differently of just doesn't look right, particularly around the area where you insert your card.

"Identity thieves attach card skimmer devices to grab your information as you're grabbing cash," Hanson says. "Sometimes you can spot them — the card insert slot looks larger or deeper than normal, and there is typically a camera."

When possible, choose an ATM that's located inside a bank. With security cameras, there's less chance that someone is lying in wait to steal your cash.

Stay alert for fraudulent charges, regularly monitor your banking and credit accounts for unauthorized transactions. This is a good tip for while you're traveling — and a good habit to adopt while you're back at home.

9. Get notified of card transactions.
While you can't prevent data breaches, the sooner you're aware of suspicious card activity, the faster you can act to stop the bleeding if you've been targeted.

For that reason, consider setting up smartphone notifications so you know when your cards are being used, suggests Rachna Ahlawat, founder and executive vice president of Ondot Systems, which makes card-tracking apps used by bank and credit union customers.

"If I'm notified every time my card is used, I'll be able to immediately detect if my card was used for a transaction I didn't authorize, and in response to that alert ... have my card switched off," she says.

10. Be prepared.
If your card is lost, stolen or otherwise compromised, make sure you have a backup card and emergency cash available, says Lightcap, who recommends using a money belt, concealed neck pouch or under-the-clothes wallet to keep your money safe when traveling to high-crime locales.

Also, make sure you have the information needed to cancel your cards, if necessary.

"I create a crib sheet which contains the overseas collect call numbers for any credit card or debit card I may be traveling with," Lightcap says. "This crib sheet is never in the same pocket as my cash or cards. In the event of loss or theft, I still have the collect numbers and can get hold of the issuer to cancel."

"As time-consuming as it can feel to make sure that all of your information is protected online and off, it's not as difficult as resolving your accounts and reclaiming your identity once it's been stolen," Schofield says. "Consumers tend not to realize that their identities have been stolen until it's too late and criminals have already taken their money and damaged their credit.

"Frequently monitoring their money, cards and financial data will help consumers catch fraud as soon as it occurs and prevent the situation from becoming any worse.

Tags: business travel, credit cards, debit cards, family finances, fraud liability, prepaid cards, security, skimmers, transaction notifications

Email Tweet Like 9 G+1 1

View Related Stories

5 good reasons to consider getting a new credit card
Thinking about adding a piece of plastic? Here are times when that may make sense...

And the credit award goes to...
From best score to best (financial) picture, learn how to walk the "good credit" red carpet with confidence...

How to manage the stages of a credit love affair
From your first date with plastic to a lasting partnership, here's how to make the most of your credit relationship...

All Credit Card News & Advice Archives

If you are commenting using a Facebook account, your profile information may be displayed with your comment depending on your privacy settings. By leaving the 'Post to Facebook' box selected, your comment will be published to your Facebook profile in addition to the space below.

Our editorial content is not sponsored by any bank or credit card issuer. The comments posted below are not provided, reviewed or approved by any company mentioned in our editorial content. Additionally, any companies mentioned in the

Credit Card Deals
Balance Transfers
0% APR
Low Interest
Cards for Business
Rewards
- Cash Back
- Gas
- Travel & Airline

Instant Approval
Cards for Students
Prepaid
Secured

Cards by Credit
Excellent Credit
Good Credit
Fair Credit
Bad Credit
Limited or No Credit History

By Matt Alderton
March 4, 2016

Email Tweet Like 9 G+1 1

Whether traveling for business or pleasure, keeping an eye on your cards and personal data is something you need to be vigilant about from airports and hotels to local restaurants.

In January, Hyatt Hotels Corp. said that 250 Hyatt hotels in 50 countries were affected by data breaches between August and December 2015. Cybercriminals used malware to steal payment card data — including cardholder names, card numbers and expiration dates. Similar breaches have occurred at hotels operated by Hilton, Starwood, Mandarin Oriental, White Lodging and Trump Hotels.

Hotels are just one worry.