



Make a Grinch Grimace

Add security to your shopping list

It's beginning to look a lot like a techie holiday. Everywhere you go there are deals on iToys, smartphones and other gadgets to place under the tree. When you're shopping for the ultimate in geek gifts, make sure your devices are secure by following these tips:

ELECTRONICS

Digital cameras—The new pocket point-and-shoots and souped-up SLRs come with more than off-the-chart megapixels and oversize LCDs. Geotagging—embedding GPS coordinates in image files—is now a standard feature. This causes trouble when sharing pictures online. Don't make an identity thief's job easy. Learn how to turn off geotagging and choose models that make that switch easy and intuitive. [Continued on page 3](#) ▶



Has Your Account Been Hijacked?

Tips to protect your online profile

Social networking and email account takeovers are a new, fast-growing form of fraud—and they're netting criminals big bucks.

Why? When they hijack a Facebook, Twitter or LinkedIn account, hackers hit more than one victim: the account holder plus all his contacts.

How it happens

Crooks get account passwords through phishing, viruses or malware. Once inside a social network account, they hit up the owner's contacts for cash. They go into his email, troll the inbox for sensitive information—such as a financial statement—and access funds. [Continued on page 4](#) ▶





What the Grinches Want This Christmas

Imagine our favorite Dr. Seuss Christmas story updated to suit the times: Instead of stuffing his giant sack with all the presents in Whoville, the Grinch pilfers electronic toys—and the information they contain.

The recession has elongated the holiday shopping season, and advertisers are appealing to our desire for the latest gadgets. From inexpensive cell phones and digital cameras to pricier devices such as tablets and e-readers, high-tech hardware is at the top of many wish lists. But criminals are adapting to new technology with the goal of separating you from your personal data. In this month's newsletter, we share tips for securing these devices.

We'll also show you what happens when hackers take over your Facebook profile. Scams that used to be limited to email are spreading to social networks, whose users often get frozen out of their own accounts.

The bad guys can even gain access to your car's computer system, but we have some road-tested solutions for you.

So whether you desire a new car or a new white iPhone, make sure security is part of your gift-giving game plan. Because unlike the Grinch, identity thieves aren't likely to catch the Christmas spirit.

As always, we hope you will enjoy.

Matt Cullina
Chief Executive Officer
Identity Theft 911

In this issue...



Features

- 5 **Modern car thieves** can hack into your car with a laptop—disabling brakes and other functions while the car is in motion. Learn how to lock thieves out.
- 6 **Case Closed:** Even though Olga Rodriguez lives in a gated community, her wallet with all her identification was stolen.

Departments

- 7 **Hail & Hiss:** A roundup of who's getting it right and wrong in the fight against identity theft and data breaches.
- 8 **Ask the Expert:** Identity Theft 911 Chief Information Security Officer Ondrej Krehel shares the latest online shopping tips.

Flash drives—Seems like everyone carries a flash drive now, from keychain danglers to models no bigger than a USB plug. They're cheap, they've got a ton of memory, but they're easy to lose. For someone who handles sensitive data, opt for a secure flash drive with onboard hardware encryption, safe password storage and the ability to run applications—like Firefox—on its own. Some models will self-destruct internally if the wrong password is entered too many times—that's reason enough for us to want one.

iToys—If you're giving the latest in iGadgets—a sure path to favorite aunt or uncle status—remind lucky recipients to use the screen lock. What's hot with Cindy Lou Who is hot with the Grinch. Thieves are as enamored with iPads and iPods as the rest of us. (A Florida man recently was arrested for stealing iPhones—and only iPhones.) Beyond the lock, there are a handful of tracking and security apps worth considering.

Laptops—Lock down those laptops—the No. 1 source of data breaches and data loss. Go low-tech: Buy a laptop lock. It's affordable and so effective that you can hit the Starbucks restroom with confidence. Go high-tech: Install drive encryption to keep hackers and cyberthieves from accessing your files if the computer is stolen. Review native software encryption programs in Windows and Mac drives. Consider hard drives with built-in, hardware-level encryption for sensitive systems.

Smartphones—They're getting smarter. But so are identity thieves. Whether you give or get a smartphone this season, look for models with a screen-lock option and use it. Minimize the use of apps that require inputting personal information. When security is a priority, opt for a BlackBerry, which encrypts calling and messaging services. And electronically engrave your device, so it can be identified if stolen and recovered.



LOW-FI

Cash—Not sure what to give? Give cash. Gift cards often come with purchasing fees, expiration dates and hidden monthly fees. The recently passed CARD Act put an end to replacement fees and short expiration dates, but there are still traps. To make matters worse, Mint.com says gift-card users are 2.5 times more likely to pay full price for their purchases. Cash is king for good reason.

Online shopping—Savvy shoppers steer clear of holiday crowds—and hackers—by shopping online safely. Use secure shopping carts—https, not http. Never save your credit card information on a retailer's site. Pay holiday bills from one financial site such as your bank webpage. Storing data in one place is safer than spreading it across a number of credit- and store-card sites.

Shredders—Shredders make excellent gifts—as long as they're cross-cut. These models turn documents with personal identifying information into confetti, not strips that can be pieced back together by enterprising thieves. •

Email addresses—the account holder’s and all his contacts’—serve as a gateway to other accounts because they’re used for authentication and communication with banks, online retailers and social networking sites.

Victims often are locked out of their accounts. The perpetrator has changed their password, security questions and other personal information. They may not be able to prove the account is theirs. Depending on the provider’s protocols, they may have to cut their losses, walk away from the account and open a new one.

Meanwhile, the victim’s contacts get hit up for money. Crooks assume the victim’s identity and send mass emails asking for cash. They tell stories of being stranded in London, Paris or Peru.

What to do

Hijacked account owners and contacts alike should sweep their computers for viruses and malware, scrutinize all accounts for changes to security questions and other options that could let hackers back in later and regularly check all online financial accounts.

Hijacked account owners who get locked out should:

- Contact the provider to explain what happened.
- Request a new username and password.
- Change all security questions.
- Consider opening a new account and inform all contacts.

Hijacked account owners who can still access their account should:

- Immediately change the password and username.
- Alert contacts.
- Check providers’ websites for recovery instructions.

Contacts and friends of hijacked account owners should:

- Never respond to unconfirmed emails from contacts requesting money.
- Print the suspicious email, then delete it.
- Inform the contact from whose account the email was sent. •



Seven ways to avoid account hijackings

1. Use different usernames and passwords for work, financial and personal accounts.
2. Use strong passwords that use numbers, symbols and upper- and lowercase letters.
3. Never store sensitive information in email.
4. Be vigilant with smartphones.
5. Avoid public wireless networks.
6. Back up your contacts; if you’re locked out, you’ll still have them.
7. Add numeric codes after answers to security questions. (For example, if your answer to the security question about your hometown is Los Angeles, then make the answer “Los Angeles 5932.”)





Dude, Where's My Smart Car?

Slim jims are so last century; today's thieves use laptops

Old-school car security: Roll up the windows, lock the doors and park in a safe place.

New-school car security: Use strong passwords, scan for malicious software and install music-encryption systems.

As vehicles become more computerized and connected to the Internet, criminals are less likely to break in than hack in by using a laptop to access a car's electronic control unit or ECU, researchers say. They can bypass security systems to mimic key codes, start engines and dismantle alarms.

In a recent [study](#), computer scientists from the University of Washington and the University of California, San Diego, demonstrated how to remotely control a car—disabling brakes, the engine and other functions—by computer.

The team tested vehicles to see what would happen if hackers gained access to the cars' networks. They were able to attack car systems by inserting malware and performing a range of functions, even while the car was moving.

A car is stolen every 33 seconds in the United States—a cost of almost \$6.4 billion a year.

— *National Insurance Crime Bureau*

Their verdict: The automotive industry should pay attention and reconsider car computer security. The researchers

didn't offer tips for how vehicles can be protected against car-hackers. But they said lessons could be learned from the PC industry, which experienced security problems after computers first became hooked up to networks.

In order for the guardian angels at OnStar to actually stop a stolen vehicle, a police report first needs to be filed. That takes time and coordination with law enforcement—time that a hacker can use to disable a GPS system.

Don't Grinch my ride

No car is theft-proof, but these steps will slow down thieves attempting to break or hack in to your vehicle.

1. **Cover the basics:** Lock your car, park in well-lit or public areas and never leave another car key anywhere in the vehicle.
2. **Consider VIN etching** on windows and engine parts so authorities can ID a car if it's stolen.
3. **Use multiple warning devices** such as car alarms, steering wheel locks and gear-shift locks.
4. **Install GPS and immobilization devices** (smart keys and kill switches).

More vehicles are built to have wireless connections, which makes them more vulnerable to hacking than old-fashioned analog cars. General Motors' OnStar system, for example, supports communications between passengers and emergency assistance and tracks a car's location. Because the system is visible to passersby, it's also considered a deterrent to crime, but more often than not it tells potential crooks exactly what system to break.

Other GPS/cellular- and radio-based tracking devices like Escort and LoJack may be better concealed and don't require lengthy police reports, but they can't shut down an engine because they aren't attached to a car's ECU.

In the end, protecting yourself and your car comes down to common sense and to making your vehicle as unappealing to auto pirates as possible. •



Gates Can't Keep Out Identity Thieves

Robbers break into exclusive community

When Olga Rodriguez moved to the gated community of Sabanera de Dorado in Puerto Rico, she thought her family would be better protected and out of harm's way.

They weren't as safe as she thought. One morning she found out that several robberies had taken place on her street. "I thought it wasn't my problem," Rodriguez said. But the next day she discovered that her house had been hit, too. The robbers had broken into her garage, found her purse in the car and emptied the wallet of cash, credit cards, her Social Security card and copies of her son's. By the time she figured out what had happened, thieves had charged \$2,000

to her bank account and tried to charge \$6,000 worth of items in California.

Rodriguez began making the requisite phone calls but described the process as "very slow." Her insurance company, Universal Insurance, put her in touch with Identity Theft 911.

Fraud specialist Joanna Gonzalez instructed Rodriguez to file a police report, reviewed her credit report and provided her with information on how and where to replace stolen identification. Gonzalez enrolled Rodriguez in Identity Theft 911's free credit monitoring

program for one year so that Rodriguez will receive alerts of suspicious activity on her accounts.

Next, Gonzalez moved to protect Rodriguez's family. She advised Rodriguez to check her 20-year-old daughter's credit on annualcreditreport.com, which is required by federal law to provide

free reports to consumers. Then she suppressed the Social Security numbers of Rodriguez's two minor children until they turn 18. That way their SSNs can't be used to open lines of credit.

"Thank goodness [Universal Insurance] put me in touch with Joanna, because everything went very fast after that, and my experience was excellent."

— Olga Rodriguez, identity theft victim

Meanwhile, Rodriguez's bank and credit issuer closed the affected accounts and opened new ones. Rodriguez was reimbursed for the lost \$2,000.

"Thank goodness [Universal] put me in touch with Joanna," Rodriguez said, "because everything went very fast after that, and my experience was excellent."

Rodriguez said she learned a tough lesson: Even in the safest neighborhoods, nothing is 100 percent secure. "Unfortunately, these days you can't be too trusting," Rodriguez said. •

Tips to outsmart the bad guys

1. Never carry Social Security cards—yours or your kids'—in your wallet.
2. Never leave a wallet or purse in the car or trunk—even if you think you've parked in a safe neighborhood.
3. Check your credit reports regularly for suspicious activity. For details, visit annualcreditreport.com.

Hail

Russian Cybercops Slam It to SpamIt.com



Moscow police shrank the global dose of unwanted Viagra ads by targeting a suspected spam kingpin. Officials investigated SpamIt.com, a company linked to billions of emails from online pharmacies hawking dubious drugs, and its alleged owner, Igor A. Gusev. He was accused of numerous crimes, including operating a pharmacy without a license. SpamIt abruptly shut its doors Sept. 27, and Gusev apparently fled Russia once the police zeroed in on his operations. Cisco Systems and Kaspersky Lab, a Moscow antivirus company, said prescription drug spam messages fell by 50 billion in the United States and Western Europe. That's a prescription for unclogging inboxes.

Unsought Oversharing: There Oughta Be a Law



Sen. Jay Rockefeller (D-W. Va.) is a fan of protecting social network users' information from going to third parties without permission. Rockefeller recently asked Facebook CEO Mark Zuckerberg and MySpace President Michael Jones for more information about breaches of private user data. His letter to Zuckerberg cautioned that the site's privacy policies affect "tens of millions" of Facebook users, whose data "could be seriously compromised." He told Jones he has "serious questions about your commitment to develop and maintain strong privacy protections for consumers." Let's see if colleagues "like" Rockefeller's legislation to protect privacy.

Brookings Shines a Light on Cloud Security Concerns



The Brookings Institution, a Washington, D.C., think tank, said neglecting security would hobble the evolution of cloud computing and called for an overhaul of outdated privacy laws. In a recent panel discussion, experts called for an update to the 24-year-old Electronic Communications Privacy Act. Data stored on personal computers has clearer legal protections than personal information stored in the cloud, which requires a level playing field. Alan Friedman, research director for the Center for Technology Innovation at Brookings, said cloud clients and vendors will have increasingly divergent interests, and that privacy needs to remain at the forefront of evolving legal and business practices.

Hiss

College Dean Gets F in Privacy



A Delaware academic administrator flunked Discretion 101 after mistakenly sending a list of 18 potentially failing pupils to every student at Wesley College. All 2,400 underclassmen got to see Dean of Students Mary Alice Ozechoski's withering comments on the academic laggards. "The hole she has dug is deeper than the mine shaft in Chile," she said of one student in danger of failing out of school. Red-faced college officials recalled the message to the listserv "StudentsMainCampus," but the school may have violated the federal Family Educational Rights and Privacy Act with its failing performance in information security.

Schmidt's Street View Comments Hit Pothole



Google CEO Eric Schmidt sent Google Street View's damage control efforts in another wrong direction when he said people can "just move" if they don't like having their houses photographed. In an appearance on CNN talk show *Parker Spitzer*, he said the global uproar over its street-level photography project wasn't about "continuous monitoring." He said people could have their home photos removed if they wanted. Tech pundits responded indignantly. *The San Francisco Chronicle* called it "an epic gaffe," and Enderle Group founder Rob Enderle said the company was joking while "flagrantly violating privacy" and was "almost begging for regulatory action."



Holiday Shopping Online? Don't get caught with your firewalls down

Q: My family is on a tight budget for the holidays. To avoid overspending, I want to do all of our shopping online. But I'm worried about hackers, viruses and scams. How can I keep my money and computer safe?

Ondrej Krehel: Online shopping is a great way to get through these post-recession holidays with your pocketbook and peace of mind intact. Items not on your shopping list stay out of sight and out of mind. Another plus? No long lines, parking jams or bad roads. Before you shop and click, protect your computer by following this checklist:

1. Install and update antivirus, anti-malware and firewall software. Update your computer's operating system and Internet browser with the latest security patches.
2. Shop on secure sites. They'll have "https" in the address bar and a yellow padlock logo to the right of the Web browser address bar.
3. Create strong passwords for online retailers and personal email accounts that have numbers, upper- and lowercase letters and symbols.
4. Use different passwords for online retailers, personal email and bank accounts. If a hacker cracks one password, he won't have access to others.
5. Read site reviews before making any purchases. Pricegrabber.com compares prices and users' comments on retail websites. Google Product Search, slickdeals.net and dealnews.com monitor retailers, site performance and possible issues.
6. Use credit cards, not debit cards. Or use a "one-time" credit card number from payment processors such as PayPal. (Some banks offer "virtual" cards. Check with yours.)
7. Never link a bank account to an online pay service such as PayPal. Hackers could break into the PayPal account and drain money from the linked bank account.

There are countless ways for criminals to exploit your personal identifying information online. But these steps will help you shop more safely.

Ondrej Krehel is chief information security officer at Identity Theft 911. Krehel manages a comprehensive information security program and leads computer forensic investigations. He helps businesses and individuals safeguard their information.