

Surviving a Hack Attack

The growth of social media and mobile technology has helped cyberthieves infiltrate business and steal employees' personal information.

Here's how to fight back.



HIGH-TECH TRENDS—INCLUDING THE

growing use of social media sites, cloud services, and

mobile devices like smartphones and tablet computers—are providing businesses with great ways to grow. They are also offering cybercrooks myriad new ways to make a killing.

“The problem is definitely growing,” says Karen Schuler, leader of the cybersecurity and information assurance practice at risk consultant Kroll

Inc., which predicts that 2012 will see a boom in cybercrime that exploits these technologies.

As an example of what can happen, Schuler points to two bank employees who were recent targets. Hackers obtained critical passwords by manipulating personal information the employees had posted on social media sites. The hackers then used the passwords to transfer \$7 million out of the bank over a period of just four hours.

While some thieves look for cash or corporate secrets, others are simply seeking personal information that can

be sold in black-market chatrooms or used for lucrative scams involving everything from bank loans to filing fraudulent tax returns to get the refunds. It's a big and growing problem. The U.S. Department of Justice says that some 8.6 million U.S. households include someone who was a victim of identity theft in 2010, an increase of more than 7% from the year before.

The impact of cyberstealth is not only big and growing; it's also widespread. A recent Kroll survey of global business leaders found information theft to be the most prevalent form



“Hi! Thanks for such a warm welcome. You’ve been quite accommodating to an outsider like me—even I was surprised at how easy it was to win your trust. Then again, that kind of trust is exactly what I bank on. Of course, I’ve become rather adept at making myself look like the trustworthy sort...you know, with system admin emails, friends’ social media posts, and the like. And now that I’m in, it’s just a matter of time before I spread across your network, wreaking havoc and stealing precious data along the way..”

Get to know your threats before they get to know your data.

- » Data Security & Privacy
- » Risk & Vulnerability Assessments
- » Data Analytics
- » Incident & Data Breach Response
- » Computer Forensics



Download Kroll’s 2012 Cyber Security Forecast and find out the top 10 trends to watch this year.

Information.Kroll.com/2012trends



Certain Altegrity companies provide investigative services. State licensing information can be found at www.altegrity.com/compliance. © 2011 Kroll, Inc. All rights reserved. Item #ADV-004-2011-1215

An Altegrity Company

of fraud, with IT complexity cited as the leading cause of increased fraud exposure.

According to the research organization Ponemon Institute, a survey of 51 U.S. companies in 15 industries showed that the number of data breaches climbed in each of the last five years, costing those businesses \$7.2 million on average in 2010. The major reason cited for the high cost is the loss of customer confidence that accompanies any theft of data.

Cyberthreats range from the physical theft of a mobile device to sophisticated malware, and new kinds of attacks are continually being developed. Ironically, the weakest security link is often the individual who inadvertently opens the door to data thieves by posting personal information online.

Keys to the Kingdom

"We know for a fact that if I can get your dog's name, your college, or your kid's name, I have a good probability of figuring out what your passwords are," says Todd Davis, CEO of LifeLock, a Tempe, Ariz., company that provides identity theft protection services to individuals. "And if I can find your name, Social Security number, and birth date, I have the keys to the kingdom."

Not surprisingly, thieves typically look for places where they can find large amounts of personal information in one spot, Davis says. That makes employers, doctors, schools, insurers, and tax accountants attractive targets.

Small businesses are also increasingly at risk, in part because they are less likely to have defensive measures in place. "You don't have to be a *Fortune* 100 company to have a target on your back," says Kröll's Schuler.

To fend off attacks, companies of all sizes need to be smarter about data protection. That starts by having a good understanding of where information is kept, says Schuler, then making sure there is adequate security to protect it. "One of the biggest mistakes companies make is failing to properly

stand guard



Keep your antivirus and software patches up to date.



Don't divulge sensitive information on social media.



Make sure corporate laptops are encrypted, and never leave a laptop unattended in a public space.



Never open unknown attachments or click on unverified e-mail links.



Use different passwords for different accounts, change passwords regularly, and make sure they contain a combination of numbers and upper- and lowercase letters.

investigate the security measures of third-party vendors," she says.

Since attacks do happen, companies also need to create incident-response plans in case a breach occurs. "If you are a small or medium-size business, you will probably not have the bandwidth to create a response team," Schuler says. But even small companies can put together a team of stakeholders to do the job, find a trusted consultant, or hire a subscription service.

Individuals can't afford to be complacent either. Davis, whose company sells an identity theft protection plan, tells of one victim who landed in jail because someone not only stole her driver's license but also committed a series of felonies. She ended up needing legal assistance and a variety of other support services before she could reclaim her identity.

The good news is that interest in identity theft protection is taking off. LifeLock currently has more than 2 million members, and a fast-growing segment of its business comes from companies offering the plan as an employee benefit.

Fact of Life

Five years from now, Davis expects, awareness of cybercrime will make data security a basic fact of life. Back in the 1950s and '60s, people commonly left their cars unlocked, often with the keys in the ignition. It won't be long, he says, before the concept of protecting your identity will become as accepted as simply locking your car. ●



Introducing your bank account's newest alarm system.



The *only* identity protection company that now monitors bank accounts for takeover fraud.

Identity thieves will stop at nothing to get at your hard earned money. They've even figured out ways to gain access to your bank accounts. All it takes are a couple pieces of information and thieves can attach a different name to your account, and make your money, their money.

Not on our watch. LifeLock has the most extensive coverage of any identity protection company. In fact, only LifeLock can now monitor member's bank accounts for changes in their personal information on existing accounts, or if someone tries to open a new account in their name. We then can quickly alert our members, *before* the damage is done.

Get the most comprehensive identity protection service you can buy.



1-800-LifeLock | LifeLock.com

*Network does not cover all transactions and scope may vary.