10 ways to protect yourself when you leave a job

Version 1.0
March 4, 2009

By Chad Perrin

In 10 important categories of employment transition security, I discussed several areas where a business should spend some time considering, developing, and implementing security measures related to employment transitions. During the transition period -- from just before an employee leaves to a few months afterward -- the organization's IT resources may be especially vulnerable.

But matters of IT security are not entirely one-sided. When you leave a job, you have similar concerns. Here's a simple list of 10 ways to help safeguard your privacy if you leave an employer for any reason. It includes some common sense advice that may seem obvious. But it's tempting to ignore such advice for the sake of convenience. Having it spelled out in a list may help remind you of the importance of these protective measures.

1 Don't violate company policies

I'm not a fan of arbitrary rules and overly restrictive behavioral policies, but that doesn't mean you should violate rules set by the employer and your immediate supervisor whenever you feel like it. Not only can this cause problems for the employer and put your job at risk, it can also give the employer more reason to invade your privacy where the law and corporate policy allow.

Remember that the more you violate company policy, the more scrutiny you're likely to attract if you get fired or laid off -- or even if you leave on what looks like good terms from your perspective. Even if they find only some minor hint of policy violations a month after you leave, it could lead to a more in-depth examination of what you left behind. In a worst-case scenario, it could potentially lead to attempts to gain legal access to information about your life outside the workplace.

2 Don't log instant messages

If you are allowed to use any of the various IM networks at work, it is best to keep any messages unrelated to work from being logged on company resources -- such as the computer on your desk. Comments made about frustration in the workplace can come back to haunt you if found lingering on the hard drive, and a laissez-faire policy in good times may turn into a fishing expedition for incriminating statements you may have made when your name comes up in the list of people to lay off. If anything suggesting misbehavior on your part comes to light, it may lead to further investigations that pry into your private communications even more. It's best to avoid leaving tracks, even if they seem innocent now, because of how they may be interpreted under other circumstances.

3 Use encryption for private communications

If company policy allows for private communications from the company network, it may be a good idea to encrypt everything so that potentially embarrassing private e-mails and IMs will not be logged by network traffic monitoring systems. Otherwise, the content of those communications may end up on some hard drive you have no control over, archived in perpetuity. Even if you have an IT department role that allows you access to the logging servers, it's best to minimize the number of places that such information gets stored in plain text.

4 Don't trust everything to encryption

While encryption tools are a great resource for protecting privacy, they are not a silver bullet. It is always possible that encrypted communications may later be decrypted, whether because the encryption scheme is cracked at some future point or because you don't have a chance to clear your encryption keys from your workstation before being escorted out of the building, allowing someone cleaning up in your wake to possibly crack your pass phrase and use the keys to decrypt your data.

Copyright © 2009 CNET Networks, Inc., a CBS Company. All rights reserved. TechRepublic is a registered trademark of CNET Networks, Inc
For more downloads and a free TechRepublic membership, please visit http://techrepublic.com.com/2001-6240-0.html

5 Don't bring your private encryption keys to work

Using public key encryption schemes, such as any of the several options for OpenPGP, is a good idea and can help ensure greater privacy in your life. You may be tempted by convenience to simply copy your encryption keys from home to your work computer, but that's a bad idea, mostly because of the previous point. Instead, you should generate a new key set at work if you want to use OpenPGP there and ensure that anyone who communicates with you via that set of keys knows that it is more subject to compromise than your more private "home" keys.

If you leave your employer, or have reason to believe the key set has been compromised (many employers still install keyloggers on company desktop computers to monitor employee behavior, after all), inform everyone who uses the public key for that set of keys to communicate with you privately that you are invalidating the key set. If you have uploaded the public key to a keyserver, you should invalidate the key on the keyserver as well.

6 Protect your private IM and e-mail passwords

It is generally best to avoid using the same IM accounts at work that you use at home, since instant messaging networks often do not encrypt login transactions between the client and the server. Just as the communications themselves may be intercepted by network traffic monitoring software, including tcpdump, so too can your user IDs and passwords for your IM accounts be intercepted -- sometimes even if the messages themselves are encrypted by some third-party plug-in.

The same can be true of e-mails, if your -email logins are not encrypted. If you employ standard UNIX mail user agents, tools such as getmail and sSMTP can help you ensure those logins are protected -- as well as the rest of the session. It is possible to use complete session encryption with Gmail, too, and GUI mail clients usually provide some mechanism for ensuring logins at least are encrypted if the server supports it. When such options are not available, though, it is best to avoid using an e-mail account you use elsewhere, just as it is with IM accounts.

7 Don't store browser history or Web site passwords not directly related to work

To the extent possible, you should ensure that you leave no tracks when browsing the Web. Many browsers, such as Firefox 3, provide a built-in password manager you can use to automate the process of entering passwords for the plethora of Web sites you may visit regularly. Some of you may not be aware that many of them -- again, like Firefox 3 -- can allow you to recover those passwords in plain text if you forget them and need to remind yourself what passwords you have used. This may allow a former employer to do the same thing after you are no longer in the office.

Browser history can be likewise problematic, allowing a glimpse further into your private habits than you may like or even serving to heighten suspicion and motivate more investigation and prying into your private life, similar to the potential effects of inferences drawn from IM logs.

8 Use encrypted proxies for private browsing

Just as you can encrypt IMs and e-mails to protect your privacy, you can also protect Web browsing from local eavesdropping at work. You can use OpenSSH as a secure Web proxy, for instance, so that all that is seen on the local network when you fire up your browser is encrypted traffic sent to a computer at your home. The advisability of this may be open to question, however, as any encrypted proxy traffic may appear suspicious to watchful net admins, and you may have to explain why you have near-constant encrypted traffic streaming to some offsite computer outside of your normal duties at work.

Copyright © 2008 CNET Networks, Inc., a CBS Company. All rights reserved. TechRepublic is a registered trademark of CNET Networks, Inc
For more downloads and a free TechRepublic membership, please visit http://techrepublic.com.com/2001-6240-0.html

9 Don't store the sole copy of anything important at work

Employers often escort employees out of the building when employment is terminated for any reason, without giving them the opportunity to recover anything from company computers. Sometimes, you may get invited to speak to a specific contact in the IT department, and have him or her recover any files you need, but that process can be long and annoying. And since it isn't their data, it may be prone to being lost somewhere along the way. Perhaps worse, any such files are likely to be scrutinized before being turned over to you, to ensure that they do not contain company secrets or otherwise present a risk to the business or its resources. It is better to ensure that anything you don't want to lose, but need to have available at work, is not stored *only* on a work computer.

10 Never give your employer reason to distrust you

Show the highest levels of integrity, even if you are angry with your employer over some deceptive behavior or other breach of trust by the employer. Do not sink to your employer's level. Don't skimp on reporting what you use, don't try to arrange surplus supplies and other resources for yourself -- don't try to get away with anything at all that might impugn your character in the eyes of the employer or any third party to which the employer may present evidence of your "misdeeds."

Even if you trust the chain of management all the way to the highest levels, in an uncertain economy it may be possible that business resources will fall to creditors, and your personal security may then be at risk. This risk can only be compounded if any evidence of your behavior can be construed by someone looking for excuses to pry into your life as justification for such an investigation. Always take pains to protect the company's security as well as your own and avoid conflicts of interest or the appearance of impropriety, to the extent reasonably possible. In times of economic desperation, in an increasingly litigious world, good intentions are often not enough to protect you.

Security across the board

Always remember that in many ways, your employer's security is also your own security, and security measures employed by someone else for his or her own benefit may prove beneficial to you, too. When it comes to security, we're all in this together. Don't let disputes over employment transition distract you from that fact.

Additional resources

- TechRepublic's Downloads RSS Feed XML
- Sign up for the Downloads at TechRepublic newsletter
- Sign up for our IT Leadership Newsletter
- Check out all of TechRepublic's free newsletters
- 10+ reasons to treat network security like home security
- 10 common security mistakes that should never be made
- 10 essential e-mail security measures

Version history

Version: 1.0
Published: March 4, 2009

Copyright © 2008 CNET Networks, Inc., a CBS Company. All rights reserved. TechRepublic is a registered trademark of CNET Networks, Inc
For more downloads and a free TechRepublic membership, please visit http://techrepublic.com.com/2001-6240-0.html

Copyright © 2008 CNET Networks, Inc., a CBS Company. All rights reserved. TechRepublic is a registered trademark of CNET Networks, Inc
For more downloads and a free TechRepublic membership, please visit http://techrepublic.com.com/2001-6240-0.html