

# Securing our eCity

## 12 Steps to Reduce Your Attack Surface

---

### At Home:

1. Buy and use a paper shredder.
  - a. Crosscut shred all documents with personally identifying information including billing statements for your Internet access, phone, cable, water, electric, etc.
  - b. Choosing a multiple sheet crosscut shredder will make thick credit applications easy to shred.
  - c. Shred anything showing you out of town at certain times.
2. Use our 'Securing Your Password' instructions.
  - a. Change your passwords today.
  - b. Educate your entire family in proper password generation.
  - c. Never give any online password to anyone, period.
3. Double your phone based security by setting a secondary password for verification.
  - a. Insist on implementing a secondary password (e.g. "bluemoon") for account access to your bank, utility company and phone company for verification of your identity over the phone. This step will foil cybercriminals who may already have partial information through a data breach.
4. Check and update your credit report often.
  - a. Do this for free at [www.annualcreditreport.com](http://www.annualcreditreport.com)
5. Carefully consider what personal information you choose to post online, e.g. Facebook.
  - a. Not everyone in your friends list may be actually your friend.
  - b. Avoid placing you out of your home at a definite time.
6. Authenticate everyone.
  - a. Do not give account passwords out, ever!
  - b. If anyone calls you unsolicited to discuss accounts, verify who they are first! Get their phone number and purpose for the call.
  - c. See if you can call them back at the company number and get transferred to their extension if you still have doubts.

## At Work:

1. Write 1 email to your HR department.
  - a. Inform them of the recent Ponemon study showing 59% of exiting employees taking company data with them.
  - b. Ask HR to review their policy on removable media after exit interviews.
2. Write 1 email to your IT department.
  - a. Ask the IT manager to review their policy on removable media access at your company.
3. Run physical security trainings.
  - a. Provide receptionist a photo directory of employees.
  - b. If your company has card-controlled access areas ensure your staff allows only one access per security card swipe.
  - c. Without card based security, ensure you have a visitor log sheet.
4. Perform a comprehensive risk assessment of your network.
  - a. If you perform credit or debit transactions, perform periodic security assessments of your internal network, wired or wireless.
  - b. Ensure employees know procedures for handling people requesting access after-hours such as passwords or information about daily routines.
5. Backup important data.
  - a. Set your employees' computers to backup automatically or require that they do it themselves.
  - b. Ensure that backups are either conducted or transported securely offsite.
6. Draft and implement a cyber security "Disaster Recovery" plan.

## Resources:

*FTC's Identity Theft Website:*

[www.ftc.gov/idtheft](http://www.ftc.gov/idtheft)

*Free Annual Credit Report:*

[www.AnnualCreditReport.com](http://www.AnnualCreditReport.com)

*United State Internet Crime Task Force:*

[www.usict.org](http://www.usict.org)

*Internet Crime Complaint Center:*

[www.ic3.gov](http://www.ic3.gov)

*Stay Safe Online:*

[www.StaySafeOnline.org](http://www.StaySafeOnline.org)

*Computer Crime Research Center:*

[www.crime-research.org](http://www.crime-research.org)

*DOJ Computer Crime & IP Section:*

[www.cybercrime.gov](http://www.cybercrime.gov)

*US-Computer Emergency Readiness Team:*

[www.us-cert.gov](http://www.us-cert.gov)