The Human Side of IT Security

Security is a shared responsibility.

People are the most valuable asset to any organization, yet human errors cause the lion's share of information security breaches.

70% of IT security breaches can be attributed to human elements.

Keep an eye out for these common pitfalls and learn what organizations and end users can do to minimize risk.

20,000-30,000 phishing attacks occur every day.

91% of targeted attacks involve spear-phishing emails

Phishing

Don't bite.

Phishing is an e-mail fraud method in which the perpetrator sends out a legitimate-looking email in an attempt to gather personal and financial information from unsuspecting recipients.

Security tips for IT

Simulate exercises to test employee knowledge of security best practices.

Have a clear, responsive reporting process in place.

Security tips for end users

Be cautious of any requests for sensitive information via email.

Know the protocol for reporting suspicious links and behaviors.

Infected websites

Think before you click.

Some trusted websites frequented by an organization's employees can be infected with malware, lying in wait for unsuspecting users.

More than 15 million new malware strains detected over three months, at an average of more than **160,000** new specimens per day.

64% of employees admitted to visiting non-work related websites every single day.

Security tips for IT

Identify logical groupings of websites and applications by category.

Inspect every packet of every piece of data coming through the environment and provide employees with secure encrypted tunnels.

Security tips for end users

Know what you're clicking on before you click on it.

Deploy security patches in a timely manner.

Passwords

Make them count.

Passwords are often the weakest link in your IT security defense, putting sensitive data and applications at risk.

76% of attacks on corporate networks involved weak passwords.

Password1 is the most commonly used password.

Security tips for IT

Enforce strong password policies and reduce the number of passwords through single sign-on.

Implement full identity lifecycle management to reduce security incidents from ungoverned user accounts or privileged users.

Security tips for end users

Create and memorize strong passwords.

Don't give out your password to anyone.

Lost and stolen devices

It happens. Be ready.

A lost or stolen device isn't just about the hardware left on the taxi seat. It's about your sensitive data out there in the world and in the wrong hands.

MISSING

27% of data breaches are due to theft or loss of devices

Average business cost of a lost laptop is **$49,246**

Security tips for IT

Deploy encryption to protect data everywhere it goes.

Secure and harden devices through regular patch management, configuration, remote and mobile management.

Security tips for end users

Never lend out a device with company or personally-identifiable data on it.

If you lose a device report it right away.

Create and promote a strong security culture

IT security technologies are only as effective as the people who use them.

Low security awareness among employees is considered the greatest inhibitor to security.

Organizations with a security awareness program are **50%** less likely to have a staff-related security breach.

Security tips for IT

Appoint an executive sponsor over security and/or hire a Chief Information Security Officer.

Conduct regular security awareness training and compliance programs.

Security tips for end users

Be a good security citizen with control over your own IT environment.

Take the time to learn from your mistakes and don't repeat them.

Ensure that people are assets, not liabilities when it comes to IT security.

People, process and technology must work together. Dell facilitates this by developing end-to-end IT security solutions that are designed to be embraced. Better security is better business.

Share your IT security story at **#BetterSecurity4All**

Learn more at **Dell.com/BetterSecurity4All**

DELL

Sources:

http://www.ponemon.org/local/upload/file/Post%20Breach%20Boom%20V7.pdf
http://www.enterprise-security-today.com/news/Human-Element-Overlooked-in-Security/story.xhtml?story_id=03100001OYS4
https://spideroak.com/privacypost/cloud-security/protection-against-phishing-attacks-in-the-cloud/
http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-spear-phishing-email-most-favored-apt-attack-bait.pdf
http://press.pandasecurity.com/news/malware-creation-breaks-all-records-in-the-first-quarter-of-2014-with-160000-new-samples-every-day//
http://www.employeepc.com/guide/employee-productivity.htm
http://www.cloudentr.com/latest-resources/industry-news/2014/3/19/weak-passwords-among-top-causes-of-data-breaches-tips-for-password-security
http://www.scmagazine.com/weak-password-trend-persists-in-the-enterprise-study-says/article/366580/
http://resources.infosecinstitute.com/2013-data-breaches-need-know/
http://www.secnap.com/support/whitepapers/laptop-loss-costs.html
http://phishme.com/phishme-reports-third-consecutive-year-extraordinary-growth/
http://www.cutimes.com/2014/04/03/your-employees-can-prevent-cyberattacks