certin
Handling Computer Security Incidents
Indian Computer Emergency Response Team
Ministry of Electronics and Information Technology
Government of India
सत्यमेव जयते

CERT-In Advisory CIAD-2016-0083

Personal Online Security

Original Issue Date: December 20, 2016

Description

Protect your email.

Email is the number one resource most of us possess. The email content can provide means to access other accounts. it is essentially your online identity. An attacker can use your email to impersonate you and try to gain access to those that trust you.

So, limit what you store in email. Don't transmit or store sensitive information, like your personally identifiable information, in your email. Imagine what it would look like to have your email published online. Try to address those concerns by removing such content from your email.

If you don't need it, delete it.

This general rule applies to applications and data. If you don't need Java or Flash or other applications on your PC, phone, or tablet, remove them. The less software on your device, the better. For data, be judicious about what you store in digital form. Anything stored on a device or in the cloud can be read, copied, changed, or deleted by an attacker.

Patch the software you keep.

If you use Windows, run a modern version and install patches regularly, for the operating system and applications. Pay attention to applications from Adobe, like Flash, Reader, and such.

Back up your data.

Research and implement a way to back up the data on your devices. Store the data in encrypted form on your laptop or PC, such that when it is stored in the cloud it is also encrypted. Enable full-device encryption on devices. Be sure you enable a numeric pin such that a thief can't simply log into your lost or stolen device. Enable services that let you remotely locate your lost or stolen device, such that you can either find them or wipe them at a distance.

Consider a password manager, but not for every Web site.

Nothing is (or should be) absolute in security. Password managers are applications that assist users with storing, supplying, and even generating usernames and passwords for Web sites and other applications. They are an improvement over using the same username and password at multiple Web sites. If you choose a password manager, select one that offers two factor authentications, such that accessing your usernames and passwords requires you to enter a numeric code. Also, don't put your most sensitive accounts in the manager.

Be careful what you download, and ask questions about the site you are downloading from.

While there are hundreds of legitimate sites from which digital content can be downloaded, there are thousands more that offer bogus, and harmful content, filled with malware designed to steal your financial and other personal information. So, if you must think twice about where you are downloading the movie or song from.

Shop safely.

If you plan to order from an online store, be sure that the Web site uses secure technology. When you are at the checkout screen, verify that the Web address begins with https. Also, check to see if a tiny locked padlock symbol appears at the bottom right of the checkout screen, or that there is a statement on the checkout screen stating that the pages are secure with a security technology vendor. Check that the security technology does exist by checking the security technology company's web site.

Pay attention to your children's online activities.

Keep your home computer in a community area so that you can monitor their activity. Use child software that is age-appropriate. Limit your children's time spent online. Install and use parental controls software that allows you to monitor your children's activity online. This will keep your children from accessing undesirable Web sites and sharing personal information via online communications.

References

CERT-In
CIAD-2016-0068: Securing Online Banking
CIAD-2016-0077: Securing Web Browsers

McAfee

https://home.mcafee.com/advicecenter/?id=ad_ost_tohtpyo

MIT
https://ist.mit.edu/security/tips

Disclaimer

The information provided herein is on "as is" basis, without warranty of any kind.

Contact Information

Email: info@cert-in.org.in
Phone: +91-11-24368572

Postal address

Indian Computer Emergency Response Team (CERT-In)
Ministry of Electronics and Information Technology
Government of India
Electronics Niketan
6, CGO Complex, Lodhi Road,
New Delhi - 110 003
India