IT@Intel Technology Tips

Intel Information Technology
November 2011

The 12 Scams of X-mas

Be aware - don't let cybercriminals ruin your holiday season

As you get ready for the holidays, be aware that cybercriminals are also preparing to take advantage of you. These crooks have scammed billions of dollars from consumers over the last few years.

Here are the 12 most dangerous online scams, as reported by McAfee.

1. Charity phishing: Donate carefully
   Hackers take advantage of seasonal generosity by sending e-mails that appear to be from legitimate charities. Instead, they are fake Web sites designed to steal your donation, credit card information, and identity.
2. Fake invoices from delivery services
   Cybercriminals often send fake invoices and delivery notifications that appear to be from nationally known shipping companies or customs offices. You may receive an e-mail asking for credit card details to credit back your account, or be asked to open an online invoice or customs form to receive a package. Once completed, your information is stolen or malware is automatically installed on your computer.
3. A cybercriminal "wants to be your friend"
   It's a social time of year. Cybercriminals take advantage of the trust-building nature of social networking by sending authentic-looking "New Friend Request" e-mails. Clicking on links in these e-mails can automatically install malware and steal personal information.

4. Holiday e-greetings

   Cyber thieves cash in on environmentally conscious or thrifty consumers who send holiday e-cards. Computer worms can come masked as a well-known retailer's seasonal promotion, or a holiday-themed video or animated e-mail attachment. Be careful what you click on.

5. "Luxury" jewelry might cost you everything

   If you think it's too good to be true, you're probably right. Don't visit malware-ridden sites offering "discounted" luxury gifts or be swayed by luxury brands. Cybercriminals may even illegally use the company's logo to trick you into buying products you'll never receive.

6. Practice safe holiday shopping to avoid online identity theft

   If you hope to take advantage of deals on the Web, be careful surfing on public hotspots. Hackers can spy on your activity in an attempt to steal your personal information. Never shop online from a public computer or on an open Wi-Fi network.

7. Searching for holiday song lyrics can be dangerous

   Hackers create fraudulent Web sites aimed at people searching for a holiday ringtone or wallpaper, Christmas carol lyrics, or a festive screensaver. Downloading holiday-themed files may infect your computer with spyware, adware, or other malware.

8. Out of work? Beware of job-related e-mail scams

   With unemployment high, scammers prey on desperate job-seekers with the promise of high-paying jobs and work-from-home opportunities. You provide personal information and pay a "set-up" fee; then hackers steal your money instead of following through on the promised employment opportunity.

9. High bid loses in online auction fraud

   Scammers often lurk on auction sites during the holiday season. Beware of auction deals that appear too good to be believed. You may never receive the item you bid on.

10. Password stealing scams

    Password theft is rampant during the holidays. Thieves use low-cost tools to uncover passwords, and then send malware to record keystrokes. Once criminals know your passwords, they can access your bank and credit card details and clean out your accounts within minutes. They also commonly send spam from a user's e-mail account to their contacts, so be on guard for strange e-mails from people you know.

11. E-mail banking scams

    Monitoring your purchases closely to stay within your holiday budget? Cybercriminals may try to trick you into divulging your bank details by sending you official-looking e-mail messages from financial institutions. They'll ask you to confirm your account information, including your user name and password, with a warning that your account will become invalid if you don't comply. This information is often sold through an online black market.

12. Your files for ransom

    Once hackers gain control of your computer through one of these holiday scams, they may hijack computer files and encrypt them, making them unreadable and inaccessible. They can then hold your files ransom, demanding payment to get them back.

With some common sense and safe computing practices, you can enjoy your holidays without putting yourself or your data at risk.

Five ways to protect your PC and personal information

- **Never click on links in e-mail messages.** Go directly to a company or charity's Web site by typing in the address or using a search engine.
- **Use updated security software.** Protect your computer from malware, spyware, viruses, and other threats with updated security suites.
- **Shop and bank on secure networks.** Check bank accounts or shop online only on secure networks at home or at work, wired or wireless. Wi-Fi networks should always be password-protected so hackers cannot gain access to them and spy on online activity. Remember to shop only on Web sites that begin with https://, instead of http://.
- **Use different passwords.** Never use the same passwords for several online accounts. Diversify passwords and use a complex combination of letters, numbers and symbols.
- **Use common sense.** If you ever doubt that an offer or product is legitimate, do not click on it. Cybercriminals are behind many of the seemingly "good" deals on the Web, so exercise caution when searching and buying.

Printed in USA Please Recycle 1111/JLG/PDF