Ransomware: It’s Not Going Away

Hackers and scammers increasingly select ransomware as their weapon of choice. According to the FBI, more than 4,000 ransomware attacks occurred every day in 2016, a 300% increase over 2015.

What is Ransomware?

One of the best definitions we have seen for ransomware comes from techtarget.com: “malware for data kidnapping, an exploit in which the attacker encrypts the victim’s data and demands payment for the decryption key.”

One of the primary delivery systems for ransomware is via phishing emails. Phishing emails containing a form of ransomware grew to over 97% during 2016.
What Can Be Done?

✓ **Install security software on all your devices.** Sophos is available to all faculty and staff, and can be downloaded from softwarelicense.arizona.edu. Protect mobile devices by downloading anti-malware from your app store.

✓ **Backup your data (twice, if possible).** Backup your data to an external hard drive and/or cloud service. Double backups provide you with peace of mind and access to your data, should your device become compromised, stolen or lost.

✓ **Don’t fall for a phish.** Phishing is ubiquitous for one reason: it’s effective. Learn how to spot a phish by visiting our phishing tips webpage, and report phishing emails to UA Information Security.

---

Tax Fraud and Identity Theft

Tax season is coming quickly. It's tax season; a stressful time for many of us, even if we are expecting refunds. That stress will multiply if your tax return gets hijacked by an identity thief.

The IRS improved some authentication processes in 2016 to help prevent tax fraud and identity theft. However, all of us must put safeguards to protect our identities and data.

**Tax Security Tips**

✓ **File early.** Tax fraud victims usually find out about a fraudulent return being filed when they go to file their return electronically, and receive a notification that their real return is a “duplicate.” By filing early, a potential thief will not be able to defraud the government in your name.

✓ **Set up two-factor authentication EVERYWHERE.** Passwords are no longer enough to protect your sensitive information. Enrolling in two-factor authentication (2fa) provides an extra layer of protection to your accounts.

✓ If a business asks for your Social Security Number, ask why it is needed. Only give this information out if it is absolutely necessary (e.g., credit reports, banking accounts).

✓ Check your credit report on a regular basis.

For more information on protecting yourself and your identity, check out our [Identity Theft](#) webpage.

---

**UA InfoSec in the News:**

- **Lo Que Pasa:** [Protect Your Identity with NetID+](#)
- **The Daily Wildcat:** [Gone phishing for data: UA fights email scams](#)
- **UA@Work:** [After Successful Phishing Scam, UA Officials Offer Tips to Stay Safe](#)

---

**PASSWORDS ARE NO LONGER ENOUGH!**

**PROTECT YOURSELF AT UA:**

ENROLL IN NetID+

---