ATF

PROTECTING THE PUBLIC
SERVING OUR NATION

TIP of the Week

Supporting the ATF Mission by Providing At-a-Glance User Assists

Avoid Phishing and Malicious Email Scams

Hackers Gonna Hack

APPROVED FOR RELEASE BY:
Walter Bigelow, Chief
Andrew Weisburger, Deputy Chief
IT Systems Management Division
Office of Science & Technology
Bureau of Alcohol, Tobacco, Firearms and Explosives

As a follow-on to the June 6th email from **Roger Beasley**, *Assistant Director, Science and Technology/CIO*, hackers are out there. While we all know what we SHOULD do, some of us still fall for fake email messages. Sophisticated attempts can fool even a mindful watcher. With that in mind, let's charge down the field boldly and use our best defenses to protect our personal systems and email.

Display Names Can Be Deceptive

Don't be fooled by just looking at the name displayed on the email. If you are not sure this is from someone you know, check the address and domain from which the email came. If you are expecting something from someone you don't know, such as a contract invoice, make sure that you check to see that it is legit from the company. You can also use PREVIEW (Reading) pane in Outlook to "see" an email without actually opening it.

"It looks like the sender is that guy in HR, I forget his last name, but I am sure it's legit." Famous last words? Well, if you were not expecting the message, it would not hurt to make a quick call to HR and see if that person actually sent it out. Is there an official signature block that is used by everyone in the office? Is there a digital signature? Was the email sent from inside the company, or from an outside source?

Bottom Line: Don't be distracted or impatient…take a moment to examine any email before you respond. For example, always hover over their email address and make sure it's the same as the name displayed.

Check that Subject Line

SENDING EMAIL: Before sending an email, you may get a pop-up message that says "The Subject Line is Blank. Send anyway?" Don't ever do that – always take time to put a relevant subject line. "From John" is not really enough of a clue to the receiver, so make it clear: "Question on Project X deliverable schedule."

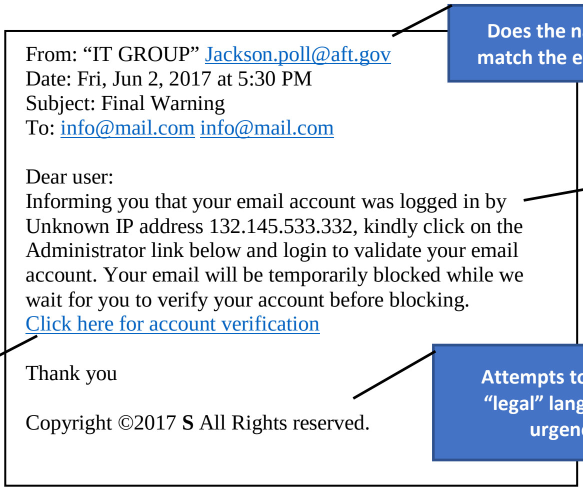
RECEIVING EMAIL: If the subject line of an incoming message seems threatening or makes you worry – such as "Account suspension unless you reply" or "Your Account has been compromised" – know that this is a common tactic for the cybercriminal.

Bottom Line: Emails with a blank subject line, or one that includes misspellings, or that uses words of fear, urgency, and despair, are the ABCs of a hacker's toolkit.

Hover, don't Click…

If there are ANY links in the email, hover your mouse over them to see where they lead. Never click directly from an email you receive unless you are completely sure it is safe.

Bottom Line: Don't click any link in an email unless you know it's legit.



From: "IT GROUP" Jackson.poll@aft.gov
Date: Fri, Jun 2, 2017 at 5:30 PM
Subject: Final Warning
To: info@mail.com info@mail.com

Dear user:
Informing you that your email account was logged in by Unknown IP address 132.145.533.332, kindly click on the Administrator link below and login to validate your email account. Your email will be temporarily blocked while we wait for you to verify your account before blocking.
Click here for account verification

Thank you

Copyright ©2017 **S** All Rights reserved.

Does the name match the email?

Lots of typos and poor grammar

Fake web address displays if you hover

Attempts to look official using "legal" language to elicit fear, urgency, or despair

Spelling and Word Use

If a big agency or professional organization sends out a mass-marketing email, it is unlikely there would be spelling errors. Companies take their branding seriously, so if you get an email that has clearly never seen a proofreader, think twice.

Bottom line: Words that emit a fear response, or a sense of urgency or despair, are the bait used to lure you in. And, the bad guys are **really bad spellers**.

Private Information

Legitimate companies don't ask for your private information via email. Passwords, credit card numbers, social security numbers – none of these should be requested or disclosed via email.

Bottom Line: Personal information shared via the Internet should be encrypted and secured; hackers don't care – they ask for private information and many times obtain it from unsuspecting, honest souls.

Seasonal and Timely Emails

Hackers and phishing scammers continue to get smarter and continually invent new methods to trick you. When the season gets hectic – such as the end of the year – they increase their efforts by sending urgent "Low-priced deals" and enticing "End-of-year Enrollment" messages. Be aware that such emails may NOT be legit – so look closely if something seems odd about it to you – don't open the message or click any links until you are sure.

Bottom Line: When our lives are busy, such as at the holiday season, hackers see this as an opportunity.

What to Do if you Spot a Bad Email

When you are using an ATF device and believe you have received a phishing email or other malicious message, forward it to: ReportSpam@atf.gov and then DELETE IT WITHOUT OPENING IT from your computer.

The Federal Trade Commission unveiled a new email address for deceptive spam – to protect American's consumers. You can forward a copy of any spam/suspicious email you receive to spam@uce.gov. You can also visit this website – Ftc.gov/idtheft – which includes free identity theft prevention tips and resources.

IdentityTheft.gov provides help to victims of identity theft. Their site provides streamlined checklists and sample letters to help you in the recovery process.

Bottom Line: Hackers gonna hack. Stop their efforts at the line of scrimmage. Be a **linebacker** – don't let them get past our best defense – **YOU**!

If you have any suggested tips, please let me know and I will share them with the community.

"Tip of the Week" *is provided to ATF users to get the most efficient use of your laptop and help you to:*

- ✓ *Become more familiar with your laptop's features as ATF moves to a more mobile environment*
- ✓ *Navigate through the new Windows 10 environment*
- ✓ *Stay updated with the latest IT news, and know where to find helpful documentation and planned outreach/learning opportunities*

"Tip of the Week" *is posted on the OST Tech Refresh Tips and Tricks website and on the ESA Services Portal (in the Communications & Outreach section). Thank you for your patience as we continue to improve the usability of our technology tools and deliver mobile computing solutions that help you accomplish your job – and the ATF mission – quickly and efficiently.*

For Assistance: *Direct questions to the **ESA IV Help Desk** by submitting a ticket via the ESA Services Portal, or you may call 877-875-3723, or send an email to:* ***Helpdesk-OSTCS@atf.gov***